



Вестник Российского университета дружбы народов. Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ

2022 Том 22 № 2

В номере: Незападный мир в киберпространстве

DOI: 10.22363/2313-0660-2022-22-2
<http://journals.rudn.ru/international-relations>

Научный журнал
Издается с 2001 г.

Издание зарегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
Свидетельство о регистрации ПИ № ФС 77-61203 от 30.03.2015 г.
Учредитель: Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов»

Главный редактор

Д.А. Дегтерев, доктор политических наук, кандидат экономических наук, профессор, РУДН, г. Москва, РФ
ir@rudn.ru

Заместитель главного редактора

К.П. Курyleв, доктор исторических наук, профессор, РУДН, г. Москва, РФ
kurylev-kp@rudn.ru

Ответственный секретарь

О.С. Чикризова, кандидат исторических наук, доцент, РУДН, г. Москва, РФ
chikrizova-os@rudn.ru

НАУЧНЫЕ РЕДАКТОРЫ:

Д.П. Елагин (экономика) (РУДН, г. Москва, РФ), кандидат исторических наук *М.М. Агазаде* (история) (РУДН, г. Москва, РФ),
М.А. Никулин (политика) (РУДН, г. Москва, РФ)

ЧЛЕНЫ РЕДАКЦИОННОЙ КОЛЛЕГИИ

Ачарья Амитаб, профессор международных отношений Школы международной службы Американского университета, г. Вашингтон, США
Беллами Алекс Дж., директор Азиатско-Тихоокеанского центра ответственности по защите, профессор по изучению проблем мира и конфликтов Университета Квинсленда (Австралия), старший советник-нерезидент Международного института мира, г. Нью-Йорк, США
Бехера Навиита Чадха, профессор кафедры политических наук Университета Дели, г. Нью-Дели, Индия
Бонд Патрик, профессор Университета Западной Капской провинции, Кейптаун, ЮАР
Воскресенский Алексей Дмитриевич, доктор политических наук, профессор кафедры востоковедения МГИМО МИД России, директор Центра комплексного китаеведения и региональных проектов, г. Москва, Российская Федерация
Жильцов Сергей Сергеевич, доктор политических наук, заведующий кафедрой политологии и политической философии Дипломатической академии МИД России, г. Москва, Российская Федерация
Иррера Даниела, доцент кафедры политических и социальных наук Университета Катании, генеральный секретарь Итальянской Ассоциации политических наук, г. Катания, Италия
Ларионова Марина Владимировна, доктор политических наук, директор Центра исследований международных институтов РАНХиГС, профессор департамента мировой экономики факультета мировой экономики и мировой политики НИУ ВШЭ, г. Москва, Российская Федерация
Маркетти Раффаэле, проректор по интернационализации, доцент международных отношений кафедры политических наук Университета ЛУИСС Гвидо Карли, г. Рим, Италия
Миттельман Джеймс, профессор Школы международной службы Американского университета, г. Вашингтон, США
Мосяков Дмитрий Валентинович, доктор исторических наук, руководитель Центра изучения стран Юго-Восточной Азии, Австралии и Океании Института востоковедения РАН, г. Москва, Российская Федерация
Мотоки Такахаси, профессор Высшей школы исследований в области международного сотрудничества Университета Кобе, президент Японского общества по международному развитию, г. Кобе, Япония
Портяков Владимир Яковлевич, доктор экономических наук, главный научный сотрудник Института Дальнего Востока РАН, г. Москва, Российская Федерация
Саква Ричард, доктор политических наук, профессор Университета Кента, г. Кентербери, Великобритания
Сапронова Марина Анатольевна, доктор исторических наук, профессор кафедры востоковедения МГИМО МИД России, г. Москва, Российская Федерация
Тикнер Арлин Б., профессор факультета политических наук, Университет Росарио, г. Богота, Колумбия
Фитуни Леонид Леонидович, член-корреспондент РАН, доктор экономических наук, заместитель директора Института Африки РАН, заведующий Центром глобальных и стратегических исследований, г. Москва, Российская Федерация
Хейфец Виктор Лазаревич, доктор исторических наук, профессор кафедры теории и истории международных отношений Санкт-Петербургского государственного университета, представитель Института Латинской Америки РАН в Санкт-Петербурге, г. Санкт-Петербург, Российская Федерация
Цыганков Андрей Павлович, кандидат философских наук, доктор философии, профессор Государственного университета Сан-Франциско, США
Чугров Сергей Владимирович, доктор социологических наук, профессор кафедры международной журналистики МГИМО МИД России, г. Москва, Российская Федерация
Шаблага Андрей Владимирович, доктор философских наук, профессор кафедры теории и истории международных отношений РУДН, г. Москва, Российская Федерация

Вестник Российского университета дружбы народов.
Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ

ISSN 2313-0679 (online); 2313-0660 (print)

4 выпуска в год, ежеквартально.

Входит в перечень рецензируемых научных изданий ВАК РФ по специальностям 5.6.7 – История международных отношений и внешней политики (исторические науки), 5.2.5 – Мировая экономика (экономические науки), 5.5.4 – Международные отношения (политические науки).

Включен в Scopus, RSCI, Ульрих (Ulrich's Periodicals Directory: <http://www.ulrichsweb.com>), базу данных Erih Plus (<https://dbh.nsd.uib.no/publiseringskanaler/erihplus/>), EBSCO.

Материалы журнала размещаются на платформе РИНЦ Российской научной электронной библиотеки, DOAJ, Electronic Journals Library Cyberleninka, Academia.Edu и Mendeley.

Языки: русский, английский.

Официальный сайт журнала: <http://journals.rudn.ru/international-relations>

Цель и тематика

«Вестник Российского университета дружбы народов. Серия: Международные отношения» — ведущий российский научный журнал, созданный в 2001 г. По своему содержанию это классический журнал по международным отношениям с особым акцентом на сотрудничество со странами СНГ, странами Глобального Юга (Азии, Африки, Латинской Америки), а также на международное образовательное сотрудничество и историю международных отношений. Журнал включен в Перечень рецензируемых научных изданий, рекомендованных ВАК РФ для публикации результатов кандидатских и докторских исследований по политическим наукам, истории и экономике. Журнал распространяется по подписке, а также рассылается в ведущие вузы РФ по международным отношениям и институты РАН. Электронный дайджест рассылается в ведущие зарубежные исследовательские центры.

Каждый из номеров имеет определенную тематическую направленность, которая задается заранее (не менее чем за 1 год). Статьи по тематике номера составляют его ядро. При этом публикуются статьи и по другим темам, в частности в постоянных рубриках журнала, к которым относятся «Мир и безопасность», «Международное экономическое сотрудничество», «Двусторонние отношения», «Международное образовательное сотрудничество». Журнал приветствует публикацию рецензий. В каждом номере в рубрике «Научные школы» размещаются академические интервью с ведущими исследователями-международниками, работающими в одной сфере, но в разных странах. Приветствуются также статьи на английском языке и статьи с выраженной исследовательской методологией, методами прикладного анализа международных отношений.

Тематический портфель на 2023 г. следующий:

Выпуск	Тема	Срок подачи краткого резюме статьи	Срок подачи полного текста статьи
№ 1 2023	Нетематический номер	До 1 сентября 2022 г.	До 15 ноября 2022 г.
№ 2 2023	Незападное миротворчество	До 1 ноября 2022 г.	До 15 января 2023 г.
№ 3 2023	100-летие Турецкой Республики	До 1 января 2023 г.	До 15 апреля 2023 г.
№ 4 2023	Международные и региональные исследования: от теории к практике	До 1 марта 2023 г.	До 15 июня 2023 г.

Правила представления рукописей размещены на сайте <http://journals.rudn.ru/international-relations>

Редактор И.Л. Панкратова

Редакторы англоязычных текстов **А.Ю. Борзова, О.С. Чикризова**

Компьютерная верстка **Н.А. Ясько**

Адрес редакции:

115419, Москва, Россия, ул. Орджоникидзе, д. 3
Тел. +7 (495) 955-07-16; e-mail: publishing@rudn.ru

Почтовый адрес редакции:

117198, Москва, Россия, ул. Миклухо-Маклая, д. 6
Тел. +7 (495) 433-03-98; e-mail: interj@rudn.ru

Подписано в печать 27.06.2022. Выход в свет 30.06.2022.

Бумага офсетная. Печать офсетная. Гарнитура «Times New Roman».

Тираж 500 экз. Заказ № 424. Цена свободная

Федеральное государственное автономное образовательное учреждение высшего образования

«Российский университет дружбы народов» (РУДН)

117198, Москва, Россия, ул. Миклухо-Маклая, д. 6

Отпечатано в типографии ИПК РУДН

115419, Москва, Россия, ул. Орджоникидзе, д. 3
Тел. +7 (495) 952-04-41; e-mail: publishing@rudn.ru



VESTNIK RUDN. INTERNATIONAL RELATIONS

2022 VOLUME 22 No. 2

In this issue: **Non-Western World in Cyberspace**

DOI: 10.22363/2313-0660-2022-22-2

<http://journals.rudn.ru/international-relations>

Founded in 2001

Founder: PEOPLES' FRIENDSHIP UNIVERSITY OF RUSSIA

EDITOR-IN-CHIEF

Professor, Dr. Denis A. Degterev
RUDN University, Moscow, Russia
ir@rudn.ru

DEPUTY EDITOR

Professor, Dr. Konstantin P. Kurylev
RUDN University, Moscow, Russia
kurylev-kp@rudn.ru

EXECUTIVE SECRETARY

PhD Olga S. Chikrizova
RUDN University, Moscow, Russia
chikrizova-os@rudn.ru

SCIENTIFIC EDITORS:

Denis N. Elagin (Economics) (RUDN University, Moscow, Russia), PhD in History *Mirmehdi M. Aghazada* (History) (RUDN University, Moscow, Russia), *Maxim A. Nikulin* (Politics) (RUDN University, Moscow, Russia)

EDITORIAL BOARD

Alex J. Bellamy, Director, Asia-Pacific Responsibility Center, Professor of Peace and Conflict Studies, University of Queensland (Australia), Senior Non-Resident Advisor, International Peace Institute, New York, USA

Alexei D. Voskressenski, Doctor of Political Sciences, Professor, Department of Oriental Studies, MGIMO University, Director, Centre for Comprehensive Chinese Studies and Regional Projects, MGIMO University, Moscow, Russian Federation

Amitav Acharya, Professor of International Relations, School of International Service, American University, Washington, USA

Andrei P. Tsygankov, PhD, Doctor of Philosophy, Professor, University of California San Francisco, San Francisco, USA

Andrei V. Shabaga, Doctor of Philosophy, Professor, Department of Theory and History of International Relations, RUDN University, Moscow, Russian Federation

Arlene B. Tickner, Professor, Department of Political Science, University of Rosario, Bogota, Colombia

Daniela Irrera, Associate Professor, Department of Political and Social Sciences, University of Catania, Secretary General of the Italian Association of Political Sciences, Catania, Italy

Dmitry V. Mosyakov, Doctor of Historical Sciences, Head, Center for Southeast Asia, Australia and Oceania, Institute of Oriental Studies, Russian Academy of Sciences, Moscow, Russian Federation

James H. Mittelman, Professor, School of International Service, American University, Washington, USA

Leonid L. Fituni, Doctor of Economics, Corresponding Member, Russian Academy of Sciences, Deputy Director, Institute for African Studies, Russian Academy of Sciences, Head, Centre for Global and International Studies, Moscow, Russian Federation

Marina A. Sapronova, Doctor of Historical Sciences, Professor, Department of Oriental Studies, MGIMO University, Moscow, Russian Federation

Marina V. Larionova, Doctor of Political Sciences, Director, Centre for International Institutions Research of Russian Presidential Academy of National Economy and Public Administration, Professor, Department of World Economy of the Faculty of World Economy and World Politics, the HSE, Moscow, Russian Federation

Navnita Chadha Behera, Professor, Department of Political Sciences, University of Delhi, New Delhi, India

Patrick Bond, Professor, University of the Western Cape, Cape Town, South African Republic

Raffaella Marchetti, Deputy Rector for Internationalization, Assistant Professor of International Relations, Department of Political Sciences, LUISS Guido Carli, Rome, Italy

Richard Sakwa, Doctor of Political Sciences, Professor, University of Kent, Canterbury, Great Britain

Sergey S. Zhiltsov, Doctor of Political Sciences, Head, Department of Political Science and Political Philosophy, Diplomatic Academy of the Ministry of Foreign Affairs of Russia, Moscow, Russian Federation

Sergey V. Chugrov, Doctor of Sociology, Professor, Department of International Journalism, MGIMO University, Moscow, Russian Federation

Takahashi Motoki, Professor, Graduate School of International Cooperation Studies, Kobe University, President of Japan Society for International Development, Kobe, Japan

Victor L. Jeifets, Doctor of Historical Sciences, Professor, Department of Theory and History of International Relations, St. Petersburg State University, Representative in St. Petersburg of the Institute of Latin American Studies, Russian Academy of Sciences, St. Petersburg, Russian Federation

Vladimir Ya. Portyakov, Doctor of Economics, Chief Researcher, Institute of Far Eastern Studies, Russian Academy of Sciences, Moscow, Russian Federation

VESTNIK RUDN. INTERNATIONAL RELATIONS
Published by the Peoples' Friendship University of Russia
(RUDN University), Moscow, Russian Federation

ISSN 2313-0679 (online); 2313-0660 (print)

Publication frequency: quarterly.

Languages: Russian, English.

Indexed in Scopus, RSCI, Ulrich's Periodicals Directory (<http://www.ulrichsweb.com>), Erih Plus database (<https://dbh.nsd.uib.no/publiseringskanaler/erihplus/>), EBSCO.

Accessible at Russian Index of Science Citation, DOAJ, Electronic Journals Library Cyberleninka, Academia.Edu, and Mendeley.

Aims and Scope

Vestnik RUDN. International Relations is a leading Russian scientific journal, established in 2001 by Peoples' Friendship University of Russia (RUDN University), which holds a top position in terms of student's body internationalization across the CIS and the BRICS (students represent more than 150 countries of the world).

This is a classic journal on international studies with a special emphasis on cooperation with the CIS countries as well as with the Global South (Asia, Africa, and Latin America), international educational cooperation and history of international relations. The journal is distributed by subscription and also on demand to leading Russian IR experts. Electronic digest is sent to the world's leading IR research centers.

The journal is international in topic coverage, editorial board and pull of authors. Being included in the international academic discourse, the journal regularly publishes articles of world recognized experts in international and regional studies from Russia, Europe, Asia and the USA. On the other hand, the edition introduces papers by promising researchers from Asia, Africa and Latin America to present their local (national, regional) vision of world that allow elaborating a balanced approach to facing global challenges.

Each of the issues has, but is not limited to a particular thematic focus, which is set in advance (at least 1 year). Articles on the thematic focus make up the "core" of issue. At the same time other topics are also covered. Constant rubrics include "Peace and Security", "International Economic Cooperation", "Bilateral Relations", and "International Academic Cooperation". The journal welcomes the publication of reviews. Academic interviews with leading researchers on international affairs, working in one area, but in different countries are allocated in every issue in the rubric "Scientific Schools".

Upcoming issues of the *Vestnik RUDN. International Relations* for 2023 will deal with the following issues:

Issue	Thematic dossier	Deadline for the abstracts	Deadline for the full texts
# 1 2023	Non-thematic Issue	By September 1, 2022	By November 15, 2022
# 2 2023	Non-Western Approaches to Peacekeeping	By November 1, 2022	By January 15, 2023
#3 2023	100th Anniversary of the Republic of Türkiye	By January 1, 2023	By April 15, 2023
#4 2023	International and Regional Studies: From Theory to Policy Science	By March 1, 2023	By June 15, 2023

Vestnik RUDN. International Relations is inviting prospective contributors. Both languages are welcome for articles — English and Russian. For more information on the thematic focus of the upcoming issues of the Journal and on the rules of submitting manuscripts, visit <http://journals.rudn.ru/international-relations>

Editor I.L. Pankratova

English text editors *A.Yu. Borzova, O.S. Chikrizova*

Computer design *N.A. Yasko*

Address of the Editorial Board:

3 Ordzhonikidze St, Moscow, 115419, Russia
Ph. +7 (495) 955-07-16; e-mail: publishing@rudn.ru

Postal Address of the Editorial Board:

10a Miklukho-Maklaya St, Moscow, 117198, Russia
Ph. +7 (495) 433-03-98; e-mail: interj@rudn.ru

Printing run 500 copies. Open price.

Peoples' Friendship University of Russia (RUDN University)
6 Miklukho-Maklaya St, Moscow, 117198, Russia

Printed at RUDN Publishing House:

3 Ordzhonikidze St, Moscow, 115419, Russia
Ph. +7 (495) 952-04-41; e-mail: publishing@rudn.ru

СОДЕРЖАНИЕ

ТЕМАТИЧЕСКОЕ ДОСЬЕ: Незападный мир в киберпространстве

- Столетов О.В.** Стратегии цифрового развития ключевых государств «Глобального Юга» в условиях американо-китайского технологического соперничества 221
- Рамич М.С., Пискунов Д.А.** Секьюритизация информационного пространства: от конструирования норм до создания правовых режимов 238
- Выходец Р.С.** Большие ИИ-пространства и стратегия России в условиях санкционной войны 256
- Cheng Guo.** China's Digital Silk Road in the Age of the Digital Economy: Political Analysis (Чэн Го. Цифровой Шелковый путь Китая в эпоху цифровой экономики: политический анализ) 271
- Pantserov K.A.** Malicious Use of Artificial Intelligence in Sub-Saharan Africa: Challenges for Pan-African Cybersecurity (Панцеров К.А. Злонамеренное использование технологий искусственного интеллекта в странах Африки южнее Сахары: вызовы panaфриканской кибербезопасности) 288
- Валиахметова Г.Н., Цуканов Л.В.** Цифровой вызов для арабского мира: фактор интеграции или дифференциации? 303
- Бабенкова С.Ю., Марьясис Д.А., Морозов В.М.** Не конфликтом единым: потенциал цифрового взаимодействия Израиля и Палестины 320

НАУЧНЫЕ ШКОЛЫ

- Международная информационная безопасность: в поисках консолидированных подходов : интервью с *Андреем Владимировичем Крутских*, Специальным представителем Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности / интервью провел Д. А. Пискунов..... 342

ПРИКЛАДНОЙ АНАЛИЗ

- Дегтерев Д.А.** Ценностный суверенитет в эпоху глобальных конвергентных медиа..... 352

МЕЖДУНАРОДНЫЕ ЭКОНОМИЧЕСКИЕ ОТНОШЕНИЯ

- Ревенко Л.С., Ревенко Н.С.** Цифровой разрыв и цифровое неравенство в продовольственных системах мира 372
- Oghuvbu E.A., Gbervbie D.E., Oni S.O.** Technology Policy and Sustainable Development in Nigeria (Огувбу Э.А., Гберевбие Д.Э., Они С.О. Технологическая политика и устойчивое развитие в Нигерии)..... 385

МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ

- Islam M.B.** Space and Counter-Space Activities of Great Powers in Outer Space (Ислам М.Б. Космическая и противокосмическая деятельность великих держав в космосе)..... 397
- Исаев Л.М., Коротаев А.В., Бобарькина Д.А.** Глобальная террористическая угроза в Сахеле и истоки терроризма в Буркина-Фасо..... 411

РЕЦЕНЗИИ

- Яникеева И.О.** Рецензия на книгу : Buchanan B. The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Cambridge, Massachusetts : Harvard University Press, 2020. 309 p. 422
- Мелконян Л.А.** Рецензия на книгу : Kharas H., McArthur J. W., Ohno I. Breakthrough: The Promise of Frontier Technologies for Sustainable Development. Brookings Institution Press, 2022. 256 p. 425
- Андреева Е.Л., Ратнер А.В.** Рецензия на книгу : Simon H. Hidden Champions: The New Game in the Chinese Century. Frankfurt — New York : Campus, 2021. 280 p. 429
- Медушевский Н.А.** Рецензия на книгу : Bhatia R. India — Africa Relations: Changing Horizons. New York : Routledge, 2021. 244 p. 433
- Кассае Ньгусие В.М.** Рецензия на книгу : Россия и Африка. Документы и материалы. 1961 — начало 1970-х / отв. ред. С.В. Мазов, А.Б. Давидсон. Москва : Политическая энциклопедия, 2021. 1006 с. 436

CONTENTS

THEMATIC DOSSIER: Non-Western World in Cyberspace

Stoletov O.V. Strategies for Digital Development of Key States of the Global South in the Context of U.S.-Chinese Technological Rivalry	221
Ramich M.S., Piskunov D.A. The Securitization of Cyberspace: From Rulemaking to Establishing Legal Regimes	238
Vykhodets R.S. Large AI Spaces and Russia's Strategy in the Context of the "Sanctions War"	256
Cheng Guo. China's Digital Silk Road in the Age of the Digital Economy: Political Analysis	271
Pantserev K.A. Malicious Use of Artificial Intelligence in Sub-Saharan Africa: Challenges for Pan-African Cybersecurity	288
Valiakhmetova G.N., Tsukanov L.V. Digital Challenge for the Arab World: Integration or Differentiation Factor?	303
Babenkova S.Yu., Mariasis D.A., Morozov V.M. Not a Conflict Only: Potential for Digital Interaction between Israel and Palestine	320

SCIENTIFIC SCHOOLS

International Information Security: In Search of Consolidated Approaches : Interview with <i>Andrey V. Krutskikh</i> , Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security. Interviewed by D. A. Piskunov	342
--	-----

APPLIED ANALYSIS

Degterev D.A. Value Sovereignty in the Era of Global Convergent Media	352
--	-----

INTERNATIONAL ECONOMIC RELATIONS

Revenko L.S., Revenko N.S. Digital Divide and Digital Inequality in Global Food Systems	372
Oghuvbu E.A., Gberevbie D.E., Oni S.O. Technology Policy and Sustainable Development in Nigeria.....	385

INTERNATIONAL SECURITY

Islam M.B. Space and Counter-Space Activities of Great Powers in Outer Space	397
Issaev L.M., Korotayev A.V., Bobarykina D.A. The Global Terrorist Threat in the Sahel and the Origins of Terrorism in Burkina Faso.....	411

BOOK REVIEWS

Yanikeeva I.O. Book review: Buchanan, B. (2020). <i>The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics</i> . Cambridge, Massachusetts: Harvard University Press, 309 p.	422
Melkonyan L.A. Book review: Kharas, H., McArthur, J. W., & Ohno, I. (2022). <i>Breakthrough: The Promise of Frontier Technologies for Sustainable Development</i> . Brookings Institution Press, 256 p.	425
Andreeva E.L., Ratner A.V. Book review: Simon, H. (2021). <i>Hidden Champions: The New Game in the Chinese Century</i> . Frankfurt — New York: Campus, 280 p.	429
Medushevsky N.A. Book review: Bhatia, R. (2021). <i>India — Africa Relations: Changing Horizons</i> . New York: Routledge, 244 p.	433
Kassaye Nigusie W.M. Book review: Mazov, S. V., & Davidson, A. B. (Eds.). (2021). <i>Russia and Africa. Documents and Materials. 1961 — early 1970s</i> . Moscow: Politicheskaya entsiklopediya publ., 1006 p. (In Russian).	436



ТЕМАТИЧЕСКОЕ ДОСЬЕ: Незападный мир в киберпространстве

THEMATIC DOSSIER: Non-Western World in Cyberspace

DOI: 10.22363/2313-0660-2022-22-2-221-237

Научная статья / Research article

Стратегии цифрового развития ключевых государств «Глобального Юга» в условиях американско-китайского технологического соперничества

О.В. Столетов  Московский государственный университет имени М.В. Ломоносова, Москва, Российская Федерация
 oleg-stoletov1@yandex.ru

Аннотация. Исследуются стратегии государств «Глобального Юга» в области осуществления цифрового развития в условиях технологического соперничества США и Китая. Дается характеристика основным особенностям американско-китайского технологического соперничества на современном этапе. Американско-китайское технологическое соперничество рассматривается как фактор, влияющий на выработку и реализацию государствами «Глобального Юга» национальных стратегий цифрового развития, предусматривающих активизацию международного сотрудничества по приоритетным направлениям. Выявляются международно-политические аспекты программ цифрового развития наиболее значимых и динамично развивающихся государств «Глобального Юга», расположенных в важных международных регионах: Юго-Восточной Азии, Южной Азии, Ближнем Востоке и Северной Африке, Африке южнее Сахары, Латинской Америке. Внимание уделяется прежде всего таким стратегическим направлениям цифрового развития рассматриваемых государств «Глобального Юга», как системы обработки и хранения цифровых данных, системы передачи цифровых данных, технологии нового поколения мобильной связи, космические программы, цифровая торговля, комплексные технологии «умный город», технологии кибербезопасности. Проанализированы стратегические подходы рассматриваемых стран «Глобального Юга» в отношении цифрового сотрудничества с США и Китаем, а также взаимодействие государств в цифровой сфере с технологически продвинутыми странами, выступающими в качестве альтернативных технологических партнеров: Японией, ведущими странами Европы, Республикой Корея, Израилем, Россией. В рамках исследования выявляются и характеризуются наиболее значимые цифровые проекты зарубежных корпораций, реализуемые совместно с рассматриваемыми странами. Изучены особенности международного сотрудничества в цифровой сфере между ключевыми странами «Глобального Юга» в рамках обозначенных в исследовании международных регионов, а также на трансрегиональном уровне. Особое внимание уделяется перспективным региональным международным технологическим проектам в цифровой сфере. Определены приоритетные направления внешнеполитической деятельности ключевых государств «Глобального Юга» с точки зрения более эффективной реализации этими государствами своих стратегий цифрового развития. Раскрываются специфические черты,

© Столетов О.В., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

присущие стратегиям цифрового развития рассматриваемых государств «Глобального Юга». Автор приходит к выводу, что эти государства в условиях американо-китайского технологического соперничества стремятся диверсифицировать свои международные связи в цифровой сфере, усилить технологический потенциал национальных цифровых компаний, укрепить национальный «цифровой суверенитет», использовать свои конкурентные преимущества для привлечения зарубежных инвестиций в цифровой сегмент национальных экономик, активизировать свой транспортно-логистический потенциал благодаря внедрению технологий Четвертой промышленной революции, расширить сотрудничество в цифровой сфере с другими странами своих международных регионов, а также на трансрегиональном уровне.

Ключевые слова: Глобальный Юг, Глобальный Север, стратегии цифрового развития, американо-китайское технологическое соперничество, гибкие международные партнерства, Индо-Тихоокеанский регион, США, Китай

Для цитирования: Столетов О. В. Стратегии цифрового развития ключевых государств «Глобального Юга» в условиях американо-китайского технологического соперничества // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 221—237. <https://doi.org/10.22363/2313-0660-2022-22-2-221-237>

Strategies for Digital Development of Key States of the Global South in the Context of U.S.-Chinese Technological Rivalry

Oleg V. Stoletov  

Moscow State University, Moscow, Russian Federation

 oleg-stoletov1@yandex.ru

Abstract. The article examines the strategies of the states of the Global South in the field of digital development in the context of technological rivalry between the United States of America and China. The main peculiarities of the U.S.-Chinese technological rivalry at the present stage are characterized. The U.S.-Chinese technological rivalry is considered as a factor influencing the development and implementation of national digital development strategies by the states of the Global South, which provide for the intensification of international cooperation in priority areas. The international political aspects of the implementation of digital development strategies of the most significant dynamically developing states of the Global South located in important international regions (Southeast Asia, South Asia, the Middle East and North Africa, Sub-Saharan Africa, Latin America) are studied. Attention is paid primarily to such strategic areas of digital development of the considered states of the Global South, as digital data processing and storage systems, digital data transmission systems, new generation mobile communication technologies, space programs, digital commerce, integrated “smart city” technologies, technologies cybersecurity. The paper explores the strategic approaches of the considered countries of the Global South in relation to digital cooperation with the United States and China. The interaction of the considered states in the digital sphere with technologically advanced countries acting as alternative technological partners (Japan, leading European countries, the Republic of Korea, Israel, Russia) is analyzed. The study identifies and characterizes the most significant digital projects of foreign corporations implemented jointly with the countries under consideration. The features of international cooperation in the digital sphere between the key countries of the Global South within the international regions defined in the study, as well as at the transregional level are analyzed. Particular attention is paid to promising regional international technological projects in the digital sphere. As a result of the study, the main priority areas of foreign policy activities of the key states of the Global South are determined from the point of view of more effective implementation by these states of their digital development strategies. The specific features inherent in the strategies of digital development of the considered states of the Global South are revealed. The author comes to the conclusion that these states, in the context of the U.S.-Chinese technological rivalry, seek to diversify their international ties in the digital sphere, strengthen the technological potential of national digital companies, strengthen national “digital sovereignty,” use their competitive advantages to attract foreign investment in the digital segment of national economies, activate their transport and logistics potential through the introduction of technologies of the Fourth Industrial Revolution, expand digital cooperation with other countries in their international regions, as well as at the transregional level.

Key words: Global South, Global North, digital development strategies, U.S.-Chinese technological rivalry, flexible international partnerships, Indo-Pacific region, USA, China

For citation: Stoletov, O. V. (2022). Strategies for digital development of key states of the Global South in the context of U.S.-Chinese technological rivalry. *Vestnik RUDN. International Relations*, 22(2), 221—237. (In Russian). <https://doi.org/10.22363/2313-0660-2022-22-2-221-237>

Введение

Современный мир переживает глубокие технологические и экономические изменения, которые оказывают воздействие на трансформацию мирового порядка (Amadi, 2020). Одним из стержневых составляющих этого процесса является стратегическое соперничество США и Китая, которое разворачивается прежде всего в технологической сфере в целом и цифровой в частности (Дегтерев, Рамич, Цвык, 2021). США и Китай реализуют политику «технологического национализма» (Kim, Lee & Kwak, 2020), которая формирует условия для технологического «декаплинга»¹. В рамках этого процесса Китай проводит политику, направленную на сокращение своей зависимости от зарубежных компаний в области производства полупроводников. В свою очередь, США, будучи крайне зависимыми от тайваньских производителей полупроводников и микросхем, также стремятся приобрести большую автономию в этой сфере (Shattuck, 2021).

Кроме того, между США и Китаем наблюдаются различия в подходах к определению юридических стандартов и этических норм в области регулирования развития цифровой сферы². Администрация президента США Дж. Байдена выдвигает идею международного партнерства «технодемократий», противостоящих «техноавтократиям», заложенную в цифровой стратегии Агентства США по международному развитию (USAID)³. Китай же продвигает концепцию

«цифрового суверенитета» (Zhao & Feng, 2021), а также выступает с инициативой «создания сообщества с единой судьбой в киберпространстве» (Дегтерев, Рамич, Пискунов, 2021).

Китайские технологические компании, реализуя свои проекты, конкурируют не только с американскими корпорациями, но и с ведущими компаниями Японии и Республики Корея. В свою очередь, основные американские технологические корпорации и цифровые компании других ведущих стран «Глобального Севера» вынуждены конкурировать не только с китайскими компаниями, но и между собой.

В рамках реализации стратегии, направленной на технологическое сдерживание КНР, США стремятся ограничить свои связи с Китаем в сфере критических технологий, вытеснить китайские цифровые компании со своего рынка и рынков своих близких военно-политических партнеров из числа стран «Глобального Севера», а также ограничить присутствие китайских цифровых компаний на перспективных рынках стран «Глобального Юга». С наибольшим давлением со стороны США сталкиваются китайские компании Huawei и ZTE. В этих условиях прослеживается нарастающая конкуренция ведущих американских (например, Meta (здесь и далее упоминается компания Meta, деятельность которой признана экстремистской по решению Тверского районного суда г. Москвы от 21.03.2022 г. и запрещена в России. — *Прим. ред.*), Google, Amazon) и китайских (например, Huawei, ZTE, Alibaba) технологических компаний за цифровые рынки государств «Глобального Юга» и формирование «цифровой геополитики» (Ефременко, 2020). В рамках этого процесса компании стремятся сформировать контролируемую ими инфраструктуру, прежде всего в стратегически значимом Индо-Тихоокеанском регионе (Okano-Neijmans & Vosse, 2021).

Технологическое соперничество США и КНР на пространстве государств «Глобального Юга» реализуется в секторах цифровой

¹ Capri A. US — China Techno-Nationalism and the Decoupling of Innovation // *The Diplomat*. September 10, 2020. URL: <https://thediplomat.com/2020/09/us-china-techno-nationalism-and-the-decoupling-of-innovation/> (accessed: 22.07.2021).

² Хунжуй Ч. Киберпространство и суверенитет. Введение в законодательство о кибербезопасности. Москва; Санкт-Петербург: Нестор-История, 2020.

³ National Security Policy // American Edge Project. February 2021. P. 1—14. URL: <https://americanedgeproject.org/wp-content/uploads/2021/02/American-Edge-Project-National-Security-Policy.pdf> (accessed: 22.07.2021).

экономки, формирующихся в парадигме Четвертой промышленной революции на глобальном уровне, в числе которых развитие технологий и инфраструктуры связи пятого поколения (5G), развитие технологий искусственного интеллекта и развитие облачных вычислений. Данная ситуация порождает прогнозы о перспективах фрагментации мира на техноэкономические блоки⁴. Тем не менее в условиях продолжающихся глобальных технологических и экономических трансформаций и сохраняющейся высокой взаимозависимости между США и Китаем цифровое будущее мира в определенной степени продолжает оставаться многовариантным, что создает для стран «Глобального Юга» определенное пространство для маневра (Atkinson, 2021).

С учетом того, что цифровые технологии являются технологиями двойного назначения, соперничество США и Китая распространяется и на военно-политическое измерение. Усиливающаяся секьюритизация сферы цифрового развития (Kulesza & Weber, 2021) оказывает прямое влияние на выработку цифровых стратегий странами «Глобального Юга», так как некоторые из этих государств находятся в различной степени военно-технологической зависимости от США и других стран «Глобального Севера». Значимым фактором, оказывающим политическое влияние на реализацию цифровых стратегий странами «Глобального Юга», является также специфика их отношений с КНР. Например, у ряда стран Юго-Восточной Азии, а также у Индии существуют территориальные споры с Китаем (Muraviev, Ahlawat & Hughes, 2021). Еще одним важным фактором, влияющим на выработку странами «Глобального Юга» стратегических подходов в области международного цифрового сотрудничества, является принадлежность этих государств к перспективным торгово-экономическим объединениям

(например, Общему рынку стран Южной Америки (МЕРКОСУР), Тихоокеанскому альянсу или Транстихоокеанскому партнерству). Большое значение для стран «Глобального Юга» имеет и то, какое место занимают Китай и США в их внешней торговле.

На уровне официальных стратегических документов страны «Глобального Юга» провозглашают курс на цифровую трансформацию, которая рассматривается ими в качестве инструмента для решения таких задач, как экономическая модернизация, повышение привлекательности своих внутренних рынков, улучшение позиций в глобальных и региональных производственно-сбытовых цепочках (Ханна, 2019). В данном исследовании представляется важным рассмотреть особенности стратегий цифрового развития ключевых государств «Глобального Юга», находящихся в основных международных регионах мира (Кузнецов, 2021). Нас прежде всего будут интересовать государства, расположенные в зонах ключевых морских маршрутов. С учетом этого обстоятельства представляется необходимым уделить особое внимание странам «Глобального Юга», среди которых Бразилия, Вьетнам, Египет, Индия, Индонезия, Мексика, Саудовская Аравия, Турция, ЮАР и др. В исследовании будут проанализированы такие стратегические направления цифрового развития рассматриваемых государств «Глобального Юга», как системы обработки и хранения цифровых данных, системы передачи цифровых данных, технологии нового поколения мобильной связи, космические программы, цифровая торговля, комплексные технологии «умный город», а также технологии кибербезопасности.

Хотя понятие «Глобальный Юг», по существу, не является географическим и вызывает в современной международно-политической науке определенные дискуссии, этот термин на данный момент является наиболее приемлемым для определения различий между развитым и развивающимся миром. Вместе с тем следует учитывать, что в условиях протекающих в настоящее время динамичных технологических и экономических изменений разделительная линия между

⁴ Безруков А. О., Мамонов М. В., Сучков М. А., Сушенцов А. А. Международная конкуренция и лидерство в цифровой среде // Международный дискуссионный клуб «Валдай». Январь 2021. С. 1—28. URL: <https://ru.valdaiclub.com/files/36581/> (дата обращения: 22.07.2021).

«Глобальным Севером» и «Глобальным Югом» зачастую проходит не только между государствами, но и внутри государств, субгосударственных регионов и даже отдельных городов (Растольцев, 2018). С этой точки зрения, мы можем относить к числу стран «Глобального Юга» государства, характеризующиеся значительными техноэкономическими, историко-политическими, культурно-цивилизационными различиями (Яковлев, 2021).

В условиях регионализации мировой политики ключевые государства «Глобального Юга», расположенные в основных международных регионах, пытаются решить сложную задачу. С одной стороны, они стремятся обеспечить достаточный уровень открытости для того, чтобы технологически развитые страны «Глобального Севера» инвестировали в развитие их экономик, способствуя интенсификации цифровой трансформации (Haider et al., 2021). С другой стороны, страны «Глобального Юга» стремятся не допустить «цифровой колонизации» (Benyera, 2021) своих экономик зарубежными технологическими компаниями, сохранив национально-государственный контроль в ключевых сегментах цифровой инфраструктуры. Таким образом, важной составляющей поведения государств «Глобального Юга» является определенного рода реагирование на продвигаемые странами «Глобального Севера» перспективные цифровые инициативы и проекты.

Основные направления цифрового развития стран «Глобального Юга»

В контексте американо-китайского технологического соперничества в мировой политике все более активно проявляется тренд на формирование так называемых «гибких» международных партнерств, в том числе в сфере цифрового сотрудничества (Bogdanov, 2019). «Гибкие» международные партнерства характеризуются рядом особенностей, в числе которых отсутствие жестких обязательств, ситуативность, то есть «собираемость под конкретные задачи» (Bogdanov, 2019), разносторонность и вариативность повестки

сотрудничества, разнообразный географический охват участников. «Гибкие» международные партнерства позволяют государствам «Глобального Юга» одновременно как конкурировать, так и сотрудничать в рамках этих партнерств. Актуализация данного тренда обусловлена как заинтересованностью США и Китая в продвижении своих интересов на более широкое пространство «Глобального Юга», так и стремлением наиболее динамично развивающихся государств «Глобального Юга» посредством реализации многовекторной политики расширить спектр своих международных партнеров в цифровой сфере. Государства «Глобального Юга», развивая разнообразные международные цифровые партнерства, в определенной степени способствуют повышению открытости международного технологического сотрудничества. Так, Объединенные Арабские Эмираты (ОАЭ), заключив в 2020 г. с Израилем договор о нормализации отношений⁵, стремятся развивать цифровое сотрудничество с этой страной, а Индия сотрудничает в цифровой сфере со странами — членами QUAD (США, Япония, Австралия).

С учетом описанной выше ситуации страны «Глобального Юга», стараясь развивать цифровое сотрудничество с США и Китаем, одновременно стремятся использовать для решения национальных задач цифрового развития формирующуюся при их участии систему «гибких» международных партнерств с третьими странами. Особое значение для государств «Глобального Юга» имеет развитие цифрового сотрудничества со странами «Глобального Севера», обладающими значительным цифровым потенциалом и в силу этого способными стать своеобразным балансиром для США и Китая. К числу таких государств «Глобального Севера» представляется возможным отнести прежде всего Японию, Республику Корея, ведущие страны Европы, Израиль и Россию.

⁵ Full Text of the Abraham Accords Signed by Israel, the UAE and Bahrain // The Times of Israel. September 16, 2020. URL: <https://www.timesofisrael.com/full-text-of-the-abraham-accords-signed-by-israel-the-uae-and-bahrain/> (accessed: 22.07.2021).

Реализация стратегий цифрового развития требует от стран «Глобального Юга» создания масштабной инфраструктуры, обеспечивающей работу с цифровыми данными. Важным элементом этой инфраструктуры являются *центры хранения и обработки данных*, обеспечивающие эффективную работу государственных и коммерческих структур в условиях цифровой трансформации. С учетом возрастания ценности любых данных, в том числе персональных, растет необходимость в обеспечении надежности хранения и скорости передачи информации в условиях развития цифровой экономики (Williams, 2021). Страны «Глобального Юга» проявляют заинтересованность в формировании инфраструктуры центров обработки данных на своей территории, внедряют принципы их локализации (Potluri, Sridhar & Rao, 2020), а также вводят правила, обязывающие технологические компании размещать данные на локальных серверах (Mansell, 2021). Решая эту задачу, страны «Глобального Юга» развивают сотрудничество с ведущими мировыми цифровыми компаниями. В частности, в 2018 г. египетская компания Telecom Egypt подписала с Huawei меморандум о создании центра обработки данных⁶. Одновременно Telecom Egypt развивает сотрудничество в области работы с цифровыми данными с нидерландской компанией AMS-IX. Нефтяная компания Саудовской Аравии Saudi Aramco сотрудничает с Google в области формирования в стране облачных центров обработки данных⁷. Ключевые страны Латинской Америки: Бразилия, Аргентина, Мексика, Чили — развивают сотрудничество в области создания центров обработки данных как с ведущими американскими компаниями (AWS, Microsoft, Google,

IBM), так и с китайской Huawei. В частности, в 2021 г. Google и IBM открыли свои «облачные регионы» на территории Бразилии в Сан-Паулу⁸.

Среди стран Юго-Восточной Азии можно выделить Таиланд, который, учитывая его выгодное географическое положение, стремится превратиться в хаб для региональной цифровой инфраструктуры. Таиланд имеет хороший потенциал для размещения на своей территории центров обработки данных, обслуживающих потребности предприятий, работающих в Юго-Восточной Азии. В частности, в рамках сотрудничества с китайской компанией Alibaba Таиланд планирует на 2022 г. запуск первого центра обработки данных⁹.

Альтернативным партнером в области создания инфраструктуры центров обработки данных для государств Юго-Восточной Азии является японская компания NTT. Индонезия демонстрирует заинтересованность в сотрудничестве с технологическими компаниями США. В 2020 г. Google открыл «облачный регион» в индонезийской Джакарте¹⁰. Индия также развивает сотрудничество с компанией Google, открывшей «облачные регионы» в Дели и Мумбаи¹¹.

⁸ См.: Stiver D. GCP Arrives in South America with Launch of São Paulo Region! // Google Cloud. September 19, 2017. URL: <https://cloud.google.com/blog/products/gcp/gcp-arrives-in-south-america-with-launch-of-sao-paulo-region> (accessed: 22.07.2021); Judge P. IBM Opens Multizone Cloud Region in Brazil // DatacenterDynamics. March 18, 2021. URL: <https://www.datacenterdynamics.com/en/news/ibm-opens-multizone-cloud-region-brazil/#:~:text=IBM%20has%20opened%20a%20multizone,offer%20customers%20reliable%20web%20services> (accessed: 22.07.2021).

⁹ Alibaba Cloud Furthers Its Commitment in Thailand by Launching Partner and Talent Initiatives // Alibaba Cloud. October 28, 2021. URL: https://www.alibabacloud.com/blog/alibaba-cloud-furthers-its-commitment-in-thailand-by-launching-partner-and-talent-initiatives_598189 (accessed: 22.07.2021).

¹⁰ Hart D. The New Google Cloud Region in Jakarta Is Now Open // Google Cloud. June 24, 2020. URL: <https://cloud.google.com/blog/products/infrastructure/new-google-cloud-region-in-jakarta-now-open> (accessed: 22.07.2021).

¹¹ Naik R. K. Google Launches Second Cloud Region in India // Analytics India Magazine. July 15, 2021. URL:

⁶ Telecom Egypt, Huawei Sign \$200M Long Term Financing Agreement // Egypttoday. May 30, 2018. URL: <https://www.egypttoday.com/Article/3/51218/Telecom-Egypt-Huawei-sign-200M-long-term-financing-agreement> (accessed: 22.07.2021).

⁷ Murphy D. Google Is Partnering with Oil Giant Aramco to Access Saudi Arabia's \$10 Billion Cloud Market // CNBC. December 23, 2020. URL: <https://www.cnbc.com/2020/12/23/google-aramco-eye-10-billion-cloud-market-in-saudi-arabia.html> (accessed: 22.07.2021).

Существенным фактором включения стран «Глобального Юга» в глобальную цифровую экономику становится развитие в этих странах современной цифровой инфраструктуры, обеспечивающей передачу электронных данных. Важным направлением международной деятельности, призванной решить эту задачу, в настоящее время является *прокладка подводных интернет-кабелей* (Bueger & Liebetau, 2021). Индия активно реализует сотрудничество с Японией в этой области. В частности, речь идет о совместных инфраструктурных проектах в области прокладки подводных интернет-кабелей, призванных обеспечить цифровую связанность между материковой частью Индии и ее островными территориями. Кроме того, японская компания NTT реализует проект прокладки подводного кабеля MIST, соединяющего ключевые порты Индии (Мумбаи и Ченнаи) с Сингапуром, Малайзией, Мьянмой, Таиландом (Iyer & Nanyam, 2021). В свою очередь, реализация индийской компанией Reliance Jio в сотрудничестве с американской компанией SubCom проекта прокладки двух новых подводных кабелей (India — Asia — Xpress и India — Europe — Xpress) призвана способствовать укреплению позиций Индии как связующего звена между странами Юго-Восточной Азии, Ближнего Востока и Северной Африки, а также государствами Европы.

Египет в настоящее время занимает ключевое транзитное положение в международной цифровой коммуникации: 17 % мировых интернет-кабелей проходят именно через его территориальные воды¹². Вместе с тем Египет прилагает усилия, направленные на сохранение своих позиций в глобальной инфраструктуре интернет-кабелей. В марте 2021 г. египетская компания Telecom Egypt представила амбициозный проект по созданию новой гибридной оптоволоконной системы *Hybrid*

<https://analyticsindiamag.com/google-launches-second-cloud-region-in-india/> (accessed: 22.07.2021).

¹² Could Egypt Make Better Use of Its Position as a Subsea Internet Cable Hub? // *Enterprise*. July 15, 2020. URL: <https://enterprise.press/stories/2020/07/15/could-egypt-make-better-use-of-its-position-as-a-subsea-internet-cable-hub-18969/> (accessed: 22.07.2021).

African Ring Path (HARP), объединяющей подводную и наземную инфраструктуру этой компании и призванной соединить Африку с Европой¹³.

Ряд африканских стран оказываются вовлечены в проекты прокладки подводных интернет-кабелей, реализуемых ведущими цифровыми корпорациями США и КНР, причем часть этих проектов являются многосторонними. В частности, проект по прокладке самого длинного подводного интернет-кабеля *2Africa* реализует консорциум, включающий в себя China Mobile International (КНР), Meta (США), MTN GlobalConnect (Южно-Африканская Республика), Orange (Франция), Telecom Egypt (Египет), Vodafone (Великобритания) и WIOCC (более десяти стран Африки). Кабель *2Africa* призван усилить цифровую связанность Африки, Европы и Азии. Еще одним важным проектом, связывающим Ближний Восток, страны Африки и Европу, стал подводный интернет-кабель *PEACE (Pakistan East Africa Connecting Europe)*, прокладкой которого занимался корпоративный консорциум во главе с китайской компанией Hengtong Group.

Страны Латинской Америки стремятся укрепить цифровые инфраструктурные связи с Азиатско-Тихоокеанским регионом. Чили в 2020 г. приняла решение реализовывать проект по прокладке первого оптоволоконного кабеля, соединяющего Южную Америку с Азиатско-Тихоокеанским регионом, совместно с Японией¹⁴. К этому проекту также присоединились Аргентина и Бразилия. В первоначальном варианте данного проекта предполагалось, что конечным пунктом назначения будет Шанхай, но в дальнейшем территория КНР была исключена из указанного проекта. Одновременно латиноамериканские страны

¹³ Menear H. Telecom Egypt's HARP to Encircle Africa with Fibre // *Mobile Magazine*. March 05, 2020. URL: <https://mobile-magazine.com/connectivity/telecom-egypts-harp-encircle-africa-fibre> (accessed: 22.07.2021).

¹⁴ Hirose Y., Toyama N. Chile Picks Japan's Trans-Pacific Cable Route in Snub to China // *Nikkei Asian*. July 29, 2020. URL: <https://asia.nikkei.com/Business/Telecommunication/Chile-picks-Japan-s-trans-Pacific-cable-route-in-snub-to-China> (accessed: 22.07.2021).

демонстрируют заинтересованность в укреплении своей цифровой инфраструктурной связанности с США. В частности, планирует участие Бразилии, Уругвая и Аргентины в проекте Google по прокладке подводного интернет-кабеля *Firmina*, соединяющего восточное побережье США с этими латиноамериканскими странами¹⁵.

Сотрудничество в области развертывания сетей мобильной связи 5G является важным аспектом стратегий цифрового развития государств «Глобального Юга». Следует отметить, что данное направление взаимодействия стран «Глобального Юга» и «Глобального Севера» проходит в рамках жесткой конкуренции американских, европейских и китайских технологических компаний. Например, в Юго-Восточной Азии Сингапур и Вьетнам с наибольшей настороженностью относятся к продвижению технологий 5G китайской компанией Huawei¹⁶. В частности, Сингапур заключил соглашение на строительство сетей 5G со шведской компанией Ericsson и финской компанией Nokia¹⁷. Вьетнам не запретил поставки продукции Huawei на свою территорию, однако вьетнамские компании избегают использовать оборудование этой китайской компании в своих сетях 5G. Малайзия также занимает осторожную позицию в отношении сотрудничества с КНР в сфере 5G. В июле 2021 г. правительство этой страны заключило контракт с компанией Ericsson на проектирование и строительство национальной сети 5G¹⁸. Тем не менее

Малайзия продолжает сотрудничать с Huawei по другим направлениям¹⁹. В свою очередь, Индонезия²⁰, Филиппины²¹ и Таиланд²² в настоящее время демонстрируют готовность развивать сотрудничество с Huawei в области сетей 5G.

Бразилия, испытывая значительное давление со стороны США, отказалась от услуг Huawei в формировании национальной сети 5G (Trevisan, 2021). По итогам проведенного в 2021 г. тендера в Бразилии победителями стали TIM Participacoes (местное подразделение итальянской компании Telecom Italia), Telefonica Brasil (бразильское подразделение испанской компании Telefonica) и бразильско-мексиканская компания Claro, входящая в состав мексиканской телекоммуникационной группы America Movil²³. В свою очередь, в Чили победителями тендера на разработку национальной сети 5G стали прежде всего национальные и другие латиноамериканские компании (Movistar, Entel, WOM, Claro), хотя оборудование для чилийской сети 5G должны будут предоставить Nokia и Huawei²⁴.

malaysia#:~:text=Ericsson%20will%20deliver%20a%20world,Malaysia%20to%20embrace%20Industry%204.0. (accessed: 22.03.2022).

¹⁵ AsiaDB, Huawei Malaysia Inks MoC to Develop Cloud-Based Digital Solutions // New Straits Times. April 18, 2022. URL: <https://www.nst.com.my/business/2022/04/789781/asiadb-huawei-malaysia-inks-moc-develop-cloud-based-digital-solutions> (accessed: 22.07.2021).

²⁰ Rakhmat M. Z., Purnama Y. For Indonesia, Chinese 5G Cooperation Brings Promise and Peril // The Diplomat. January 20, 2021. URL: <https://thediplomat.com/2021/01/for-indonesia-chinese-5g-cooperation-brings-promise-and-peril/> (accessed: 22.02.2022).

²¹ Cuyegkeng S. 5G Geopolitics and the Philippines: The Huawei Controversy // Asia Pacific Foundation of Canada. December 22, 2021. URL: <https://www.asiapacific.ca/publication/5g-geopolitics-and-philippines-huawei-controversy> (accessed: 22.02.2022).

²² Janssen P. Huawei On a 5G Roll in US Ally Thailand // Asia Times. January 7, 2022. URL: <https://asiatimes.com/2022/01/huawei-on-a-5g-roll-in-us-ally-thailand/> (accessed: 22.02.2022).

²³ Lennighan M. Brazil Finally Gets Its 5G Act Together // Telecoms.com. November 5, 2021. URL: <https://telecoms.com/512058/brazil-finally-gets-its-5g-act-together/> (accessed: 21.02.2022).

²⁴ Chile Completes First 5G Spectrum Auction in Latin America // European 5G Observatory. March 18, 2021. URL: <https://5gobservatory.eu/chile-completes-first-5g-spectrum-auction-in-latin-america/> (accessed: 21.02.2022).

¹⁵ Koley B. Hola, South America! Announcing the Firmina Subsea Cable // Google Cloud. June 9, 2021. URL: <https://cloud.google.com/blog/products/infrastructure/announcing-the-firmina-subsea-cable> (accessed: 22.09.2021).

¹⁶ Sacks D. China's Huawei Is Winning the 5G Race. Here's What the United States Should Do to Respond // Council on Foreign Relations. March 29, 2021. URL: <https://www.cfr.org/blog/china-huawei-5g> (accessed: 22.07.2021).

¹⁷ Singapore Telecoms Operators Select Nokia, Ericsson to Build 5G Networks // Reuters. June 24, 2020. URL: <https://www.reuters.com/article/singapore-telecoms-5g-idINKBN23V10A> (accessed: 22.07.2021).

¹⁸ Media Statement on Ericsson's Contract to Deploy 5G for Malaysia // Ericsson. March 03, 2022. URL: <https://www.ericsson.com/en/press-releases/2/2022/3/media-statement-on-ericssons-contract-to-deploy-5g-for->

Страны Африки южнее Сахары, будучи зависимыми от европейских и американских компаний-поставщиков интернет-услуг, тем не менее, стремятся развивать сотрудничество в области 5G с Китаем (Панцеров, 2019). ЮАР и Кения стали первыми странами региона, которые предоставили китайской компании Huawei возможность построить на их территории автономные коммерческие сети 5G²⁵.

Важным направлением в реализации стратегий цифрового развития стран «Глобального Юга» является *развитие международной кооперации в сфере освоения космоса и реализация национальных космических программ*. Наглядной иллюстрацией этого процесса в последние несколько лет стало создание национальных космических агентств в Египте, ОАЭ, Саудовской Аравии и Турции. Страны Ближнего Востока развивают сотрудничество в космической сфере с США, Россией и Францией. Страны Юго-Восточной Азии в настоящее время сотрудничают в области реализации своих космических программ, прежде всего с США, Францией и Японией. При этом Вьетнам видит Россию в качестве перспективного партнера в области освоения космоса. На уровне двусторонних отношений достигнуто стратегическое намерение сотрудничать в сфере использования и развития глобальной навигационной системы ГЛОНАСС²⁶. Кроме того, страны Юго-Восточной Азии участвуют в работе региональных многосторонних международных объединений в сфере космической деятельности. Речь идет о международном взаимодействии в рамках двух структур — Азиатско-Тихоокеанского регионального форума космических агентств (APRSAF), учрежденного

в 1993 г. по инициативе Японии, и Азиатско-Тихоокеанской организации по космическому сотрудничеству (APSCO), созданной Китаем в 2005 г. В последнюю, помимо КНР, входят Таиланд, Монголия, Бангладеш, Пакистан, Иран, Перу и Турция (Yan, 2021). В связи с этим представляется возможным говорить о наличии тенденции к усилению международной конкуренции в космической сфере в Индо-Тихоокеанском регионе (Nie, 2019).

Африканские государства видят для себя перспективным взаимодействие с Китаем в сфере космических технологий. Так, в ноябре 2021 г. состоялся Первый Китайско-Африканский форум по сотрудничеству в области навигационной спутниковой системы BeiDou²⁷. Страны Африканского континента намерены использовать китайскую систему BeiDou для решения задач социально-экономического и экологического развития. При этом африканские государства, опираясь на интеграционный потенциал Африканского союза, стремятся развивать общеконтинентальное взаимодействие в области освоения космоса. Реализуя стратегию «Повестка дня 2063», африканские страны достигли взаимопонимания по вопросу создания Африканского космического агентства, которое будет базироваться на территории Египта²⁸.

В Латинской Америке также наметились предпосылки к развитию макрорегиональной кооперации в космической сфере. По инициативе Мексики и Аргентины в сентябре 2020 г. ряд стран Латинской Америки подписали Конвенцию об учреждении Космического агентства Латинской Америки и Карибского бассейна, а в июле 2021 г. шесть латиноамериканских стран (Мексика, Аргентина, Боливия, Коста-Рика, Эквадор и Парагвай) заключили соглашение о создании Космического агентства Латинской Америки и Карибского

²⁵ Huawei Technologies: A Chinese Trail Blazer in Africa // Knowledge at Wharton. April 20, 2009. URL: <https://knowledge.wharton.upenn.edu/article/huawei-technologies-a-chinese-trail-blazer-in-africa/> (accessed: 21.02.2022).

²⁶ Россия и Вьетнам намерены сотрудничать в использовании и развитии ГНСС ГЛОНАСС // Вестник ГЛОНАСС. 01.12.2021. URL: http://vestnik-glonass.ru/news/vo_vlasti/rossiya-i-vietnam-namereny-sotrudnichat-v-ispolzovanii-i-razvitii-gnss-glonass/ (дата обращения: 22.02.2022).

²⁷ The First China — Africa BDS Cooperation Forum Held in Beijing // Embassy of the People's Republic of China in the Republic of South Africa. November 10, 2021. URL: http://za.china-embassy.org/eng/sgxw/202111/t20211110_10446583.htm (accessed: 22.02.2022).

²⁸ Statute of the African Space Agency // African Union Commission. January 29, 2018. URL: https://au.int/sites/default/files/treaties/36198-treaty-statute_african_space_agency_e.pdf (accessed: 22.02.2022).

бассейна²⁹. Параллельно ряд стран Африки и Латинской Америки инициировали подписание с Россией рамочных документов о развитии сотрудничества в космосе. В частности, в декабре 2020 г. вступил в силу федеральный закон «О ратификации Протокола между Правительством Российской Федерации и Правительством Аргентинской Республики о сотрудничестве в области исследования и использования космического пространства в мирных целях»³⁰. Запланирована реализация совместных проектов по установке на территории Аргентины наземных станций ГЛОНАСС, оптико-электронного комплекса для предупреждения об опасных ситуациях в околоземном космическом пространстве, а также оказанию пусковых услуг и совместному созданию космической техники. Индия, обладающая собственной региональной навигационной спутниковой системой (NavIC), в рамках сотрудничества с Россией планирует разместить на российской территории наземные станции своих навигационных систем, предоставив России возможность разместить на своей территории системы ГЛОНАСС (Santra et al., 2019).

С учетом того, что во многих странах «Глобального Юга» в настоящее время формируются перспективные капиталоемкие потребительские рынки, эти государства прилагают усилия, направленные на *развитие международного сотрудничества в сфере цифровой торговли*. Среди динамично развивающихся стран Юго-Восточной Азии особенно выделяется Вьетнам, который стремится к тому, чтобы в перспективе играть

²⁹ Volterra R. G., Tuma R. G. Latin America and the Caribbean Join the Space Race with the Creation of a Regional Space Agency (ALCE) // Mondaq. October 27, 2021. URL: <https://www.mondaq.com/uk/technology/1124938/latin-america-and-the-caribbean-join-the-space-race-with-the-creation-of-a-regional-space-agency-alce> (accessed: 22.02.2022).

³⁰ О Федеральном законе «О ратификации Протокола между Правительством Российской Федерации и Правительством Аргентинской Республики о сотрудничестве в области исследования и использования космического пространства в мирных целях» // Совет Федерации Федерального Собрания Российской Федерации. 02.12.2020. URL: <http://council.gov.ru/activity/documents/121937/> (дата обращения: 08.01.2022).

более активную роль в выработке правил цифровой торговли как на уровне Всемирной торговой организации, так и на региональном уровне (Kim, 2019). В рамках решения этой задачи Вьетнам в июне 2021 г. договорился с Сингапуром о создании совместной рабочей группы по цифровому партнерству, призванной изучить возможности разработки двустороннего соглашения о цифровой экономике³¹. Вьетнам также развивает сотрудничество в сфере электронной торговли с американской компанией Amazon³².

Важным направлением развития электронной торговли латиноамериканских стран является сотрудничество по линии «Юг — Юг». Бразилия способствует развитию кооперации в области электронной торговли в рамках МЕРКОСУР, в том числе в целях решения задач региональной экономической интеграции (Коваль, Андрианова, 2020). В свою очередь, Мексика поддерживает формирование регионального цифрового рынка в рамках Тихоокеанского альянса, внутри которого была разработана дорожная карта в области «цифровой повестки дня»³³.

Существуют перспективы подключения государств Азиатско-Тихоокеанского региона, участвующих в Транстихоокеанском партнерстве, к возможному соглашению о цифровой торговле с участием США и других государств «Глобального Севера», расположенных в Азиатско-Тихоокеанском регионе и являющихся союзниками США³⁴.

³¹ Singapore, Vietnam to Work on Digital Economy Agreements // The Strait Times. June 22, 2021. URL: <https://www.straitstimes.com/asia/se-asia/singapore-vietnam-to-set-up-working-groups-to-develop-agreements-on-digital-economy> (accessed: 22.02.2022).

³² Phuong H. Amazon Announced to Strengthen Collaboration with iDEA // Vietnam Investment Review. April 28, 2021. URL: <https://vir.com.vn/amazon-announced-to-strengthen-collaboration-with-idea-83931.html> (accessed: 22.07.2021).

³³ Pacific Alliance's Digital Agenda // Alianza del Pacifico. 2022. URL: <https://alianzapacifico.net/en/technical-group-digital-agenda/#:~:text=During%20the%2011th%20Pacific%20Alliance,what%20is%20established%20in%20the> (accessed: 22.02.2022).

³⁴ The US Appears Poised to Pursue a Digital Trade Agreement in Asia — What Does that Mean? // Steptoe & Johnson LLP. October 15, 2021. URL:

Предполагается, что новое соглашение может базироваться на тех соглашениях в области цифровой торговли, которые ранее были заключены между США и Японией, Сингапуром и Австралией, а также Сингапуром, Новой Зеландией и Чили.

Индия, реализуя Национальную стратегию финансовой инклюзии на 2019—2024 гг., развивает сектор цифровых финансовых технологий, рассматривая его в качестве инструмента раскрытия потенциала внутреннего рынка, обеспечивающего вовлечение граждан страны в эффективную экономическую деятельность (Кириченко, 2021). Саудовская Аравия стремится активизировать развитие цифровой торговли между странами Ближнего Востока, соседних регионов и Африки посредством созданной в 2020 г. Организации цифрового сотрудничества, в которую, наряду с Саудовской Аравией, вошли Бахрейн, Кувейт, Иордания, Пакистан, Оман и Нигерия.

Важным аспектом глобальной цифровой конкуренции не только государств «Глобального Юга», но и отдельных территорий этих государств является *внедрение комплексных технологий «умный город»* (Ross, Banerjee & Chowdhury, 2020). В частности, Индия с 2015 г. реализует программу «Миссия 100 умных городов»³⁵. Выполнение данной программы помогло заинтересовать инвесторов и внедрить технологии из таких стран, как США, Великобритания, Франция и Израиль (Перминов, 2020). Кроме того, Индия осуществляет сотрудничество с российской компанией NtechLab, разрабатывающей программные решения для видеоаналитики, обеспечивающие функционирование видеокamer с функцией распознавания лиц. В частности, на Западной железной дороге в Индии были установлены системы видеоаналитики

<https://www.steptoeglobaltradeblog.com/2021/10/the-us-appears-poised-to-pursue-a-digital-trade-agreement-in-asia-what-does-that-mean/> (accessed: 22.02.2022).

³⁵ Smart Cities. Mission Statement & Guidelines // Government of India. June 2015. URL: [https://web.archive.org/web/20170801155633/http://164.100.161.224/upload/uploadfiles/files/SmartCityGuidelines\(1\).pdf](https://web.archive.org/web/20170801155633/http://164.100.161.224/upload/uploadfiles/files/SmartCityGuidelines(1).pdf) (accessed: 22.02.2022).

NtechLab на 30 железнодорожных станциях между западно-индийскими штатами Гуджарат и Махараштра, включая Мумбаи³⁶.

Страны АСЕАН стремятся к активному внедрению технологий «умный город» на своей территории (Kong & Woods, 2021), в том числе с привлечением ведущих зарубежных цифровых компаний. Индонезия сотрудничает с китайской Huawei, например, в рамках реализации проекта «умный город» в Бандунге³⁷. Филиппины и Вьетнам развивают взаимодействие с технологическими компаниями Японии и Республики Корея. Кроме того, в мае 2019 г. Вьетнам заключил соглашение с Россией о поставке на свой рынок российских IT-решений в области электронного правительства, информационной безопасности и «умного города». В рамках достигнутой договоренности были заключены соглашения между ведущим поставщиком телекоммуникационных и IT-услуг Вьетнама Vietnam Posts and Telecommunications Group (VNPT) и российскими компаниями «Ростелеком», «Альтарикс», Kaspersky Lab, FORS и Netris³⁸.

Внедрение технологий «умный город» осуществляют и страны Ближнего Востока — Египет, Турция, Саудовская Аравия и Катар. Египет развивает сотрудничество в области внедрения технологий «умный город» с французской компанией Orange. Турция взаимодействует в этой области с Агентством США по торговле и развитию (USTDA). В 2020 г. USTDA запустило американо-турецкую инициативу «Города следующего поколения», призванную содействовать внедрению технологий «умный город» на

³⁶ Железные дороги Индии начали применять российскую технологию распознавания лиц // ТАСС. 26.08.2021. URL: <https://tass.ru/ekonomika/12222333> (дата обращения: 08.01.2022).

³⁷ Innovative ICT to a Better Connected Smart City: Huawei and PT. PINS Indonesia Collaborate to Develop Smart City Project in Bandung // Huawei. April 3, 2015. URL: https://www.huawei.com/en/news/2015/04/hw_422361 (accessed: 22.07.2021).

³⁸ РФ поставит во Вьетнам «умный город» и электронное правительство // Российская газета. 22.05.2019. URL: <https://rg.ru/2019/05/22/rf-postavit-vo-vietnam-umnyj-gorod-i-elektronnoe-pravitelstvo.html> (дата обращения: 08.01.2022).

территории Турции³⁹. Другая ближневосточная страна — Саудовская Аравия — стремится позиционировать себя в качестве активного драйвера цифровой трансформации в регионе. Совместно с ведущими мировыми технологическими корпорациями саудовская компания Neom Tech & Digital Company реализует проект по созданию крупнейшего плавающего промышленного комплекса «Оксагон». В частности, американская цифровая корпорация Oracle планирует разместить на территории комплекса «Оксагон» облачный центр хранения и обработки данных⁴⁰. При этом, внедряя в городе Янбу технологии «умный город», Саудовская Аравия привлекала китайскую компанию Huawei⁴¹. В свою очередь, Катар реализует программу Tasmu Smart Qatar совместно с Microsoft Qatar⁴².

В связи с тем, что цифровое развитие напрямую связано с умножением разнообразных технологических уязвимостей, а в мире возрастает интенсивность кибератак, страны «Глобального Юга» уделяют все большее внимание *проблематике киберугроз*. В частности, Мексика утвердила Национальную стратегию кибербезопасности в 2017 г.⁴³, а

³⁹ USTDA Announces U.S. — Turkey Next Generation Cities Initiative // U.S. Embassy and Consulates in Turkey. June 29, 2020. URL: <https://tr.usembassy.gov/ustda-announces-u-s-turkey-next-generation-cities-initiative/> (accessed: 22.07.2021).

⁴⁰ Neom Announces Oxagon Floating Industrial District That Will House Data Center // DCD. November 19, 2021. URL: <https://www.datacenterdynamics.com/en/news/neom-announces-oxagon-floating-industrial-district-that-will-house-data-center/> (accessed: 22.07.2021).

⁴¹ Providing a Secure and Efficient Traffic Environment for Yanbu, Saudi Arabia, with Huawei's ITMS // Huawei. 2020. URL: <https://e.huawei.com/en/case-studies/industries/government/2020/traffic-management-solution-yanbu> (accessed: 22.07.2021).

⁴² Microsoft Technologies Power Up TASMU Platform, the World's Most Innovative Cloud-based Smart City Solution // Microsoft News Center. July 27, 2021. URL: <https://news.microsoft.com/en-xm/2021/07/27/microsoft-technologies-power-up-tasmu-platform-the-worlds-most-innovative-cloud-based-smart-city-solution/> (accessed: 22.07.2021).

⁴³ National Cybersecurity Strategy of Mexico // Gobierno de México. 2017. URL: <https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf> (accessed: 22.07.2021).

Бразилия — в 2020 г.⁴⁴ В стратегии кибербезопасности Мексики сделан акцент на необходимости усиления международного взаимодействия в области кибербезопасности, в том числе в целях повышения качества обеспечения национальной безопасности. Что касается Бразилии, то она подчеркивает важность развития международного сотрудничества в области кибербезопасности с максимально возможным количеством стран мира посредством расширения сотрудничества со странами Латинской Америки.

Страны АСЕАН стремятся укреплять свой потенциал в области кибербезопасности, в том числе в рамках международного сотрудничества. Сингапур подписал двусторонние соглашения о сотрудничестве в области кибербезопасности с Австралией, Канадой, Эстонией, Францией, Германией, Индией, Японией, Нидерландами, Великобританией и США. В августе 2019 г. государственные структуры Вьетнама заключили контракт с российской компанией «Лаборатория Касперского»⁴⁵. Достаточно активно наращивает потенциал кибербезопасности Малайзия. В 2020 г. на территории этой страны был открыт совместный австрийско-малайзийский центр компетенций в области информационных технологий и безопасности данных⁴⁶. Вместе с тем Малайзия в 2021 г. объявила о создании совместно с компанией Huawei лаборатории, которая займется вопросами обеспечения кибербезопасности сетей 5G⁴⁷.

⁴⁴ Estratégia Nacional de Segurança Cibernética // Portal da Imprensa Nacional. February 5, 2020. URL: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419> (accessed: 22.07.2021).

⁴⁵ «Лаборатория Касперского» займется созданием антивирусов для властей Вьетнама // Ведомости. 07.08.2019. URL: <https://www.vedomosti.ru/technology/news/2019/08/07/808321-laboratoriya-kasperskogo-vietnam> (дата обращения: 08.01.2022).

⁴⁶ TÜV AUSTRIA Cybersecurity Lab Official Launch in Malaysia // Advantage Austria. January 20, 2021. URL: https://www.advantageaustria.org/my/news/TUeV_AUSTRIA_Group_and_Malaysian_LGMS_.en.html (accessed: 22.07.2021).

⁴⁷ Lee J. The Internet of Things: China's Rise and Australia's Choices // Lowy Institute. December 8, 2021. URL: <https://www.lowyinstitute.org/publications/>

В свою очередь, базирующаяся в Дубае компания Spire Solution, специализирующаяся в области кибербезопасности, в 2021 г. заключила соглашение о сотрудничестве с работающей в этом сегменте цифрового рынка израильской компанией ХМ Cyber⁴⁸.

Кибербезопасность представляет собой сферу, в которой для стран «Глобального Юга» особое значение имеет сотрудничество с Россией. Такие страны Юго-Восточной Азии, как Вьетнам и Индонезия, демонстрируют намерение развивать партнерство в области кибербезопасности с Российской Федерацией. Индия, сталкиваясь с серьезными угрозами в киберпространстве⁴⁹, в настоящее время завершает разработку национальной стратегии кибербезопасности. Индийская группа реагирования на компьютерные чрезвычайные ситуации (CERT-In) осуществляет сотрудничество с компанией «Лаборатория Касперского»⁵⁰. Одновременно Индия демонстрирует заинтересованность в сотрудничестве в сфере кибербезопасности со странами QUAD и АСЕАН. Малайзия разместила у себя региональный офис «Лаборатории Касперского» в 2008 г.⁵¹, а ЮАР — в 2009 г.⁵²

the-internet-of-things-chinas-rise-and-australias-choices (accessed: 22.07.2021).

⁴⁸ ХМ Cyber Partners with Spire Solutions to Offer Its Solutions in The Middle Eastern Market // Help Net Security. May 11, 2021. URL: <https://www.helpnetsecurity.com/2021/05/11/xm-cyber-spire-solutions/> (accessed: 22.07.2021).

⁴⁹ Куприянов А. В. Индия в эпоху кибервойн // Российский совет по международным делам. 07.08.2019. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/indiya-v-epokhu-kibervoyzn/> (дата обращения: 08.01.2022).

⁵⁰ Abraham R. Kaspersky Joins Hands with CERT-In to Keep Cyber Threats at Bay, Focus on Privacy Protection // The Economic Times. December 2, 2020. URL: <https://economictimes.indiatimes.com/magazines/panache/kaspersky-joins-hands-with-cert-in-to-keep-cyber-threats-at-bay-focus-on-privacy-protection/articleshow/79529391.cms> (accessed: 22.07.2021).

⁵¹ «Лаборатория Касперского» открывает офис в Юго-Восточной Азии // РИА Новости. 08.10.2008. URL: <https://ria.ru/20081008/152789378.html> (дата обращения: 08.01.2022).

⁵² «Лаборатория Касперского» открыла офис в ЮАР // РИА Новости. 20.11.2009. URL: <https://ria.ru/20091120/194724571.html> (дата обращения: 08.01.2022).

Заключение

Страны «Глобального Юга» подошли к фазе обострения американо-китайского соперничества с различными стартовыми позициями в цифровой сфере. Индия, как страна, обладающая значительным потенциалом, занимающая стратегическое положение в Индо-Тихоокеанском регионе и имеющая глобальные амбиции, стремится развивать цифровые партнерства с технологически продвинутыми государствами, в числе которых США, Япония, Франция, Великобритания, Израиль и Россия. Государства АСЕАН, прежде всего расположенные в зоне Малаккского пролива, осознают свою значимость для США и их союзников в Индо-Тихоокеанском регионе и потому демонстрируют определенную уверенность в перспективности выстраивания международных цифровых партнерств на многовекторной основе.

Страны Ближнего Востока, исторически игравшие важную роль на пространстве Шелкового пути наряду со странами Юго-Восточной Азии, в настоящее время демонстрируют заинтересованность в том, чтобы принять активное участие в формировании цифровой связанности Индо-Тихоокеанского региона, в которой будут учитываться как интересы Китая и Индии, так и интересы других ведущих международных акторов. Арабские монархии Персидского залива, прежде всего Саудовская Аравия и ОАЭ, в условиях усиления американо-китайского технологического соперничества стремятся проводить политику стратегического хеджирования рисков. Занимая сбалансированную позицию, страны Ближнего Востока развивают цифровое сотрудничество с КНР, однако при этом формируют систему цифровых партнерств с ведущими странами Европы, Израилем и Россией.

Государства Африки южнее Сахары, рассматривающие цифровую трансформацию как исторический шанс для себя преодолеть многолетнее экономическое и технологическое отставание, демонстрируют готовность не только продолжать, но и расширять сотрудничество в цифровой сфере с Китаем. В свою очередь, государства Латинской Америки, будучи экономически тесно связаны с

рынком США и испытывая на себе их политическое давление, вынуждены подходить к цифровому сотрудничеству с китайскими компаниями со все большей осторожностью, преимущественно развивая отношения в этой сфере с технологическими компаниями США, европейских государств и Японии.

Американо-китайское стратегическое соперничество имеет сложную природу, которую страны «Глобального Юга» пытаются учитывать. Конкурируя между собой, США и Китай вносят определенный вклад в технологическую модернизацию стран «Глобального Юга». В свою очередь, страны «Глобального Юга», реализуя стратегии цифрового развития в условиях стратегического соперничества США и Китая, стремятся получить как от американских, так и от китайских цифровых корпораций доступ к наиболее передовым технологическим решениям в сфере цифровой экономики, в том числе для того, чтобы на основе этих решений повысить уровень собственного «цифрового суверенитета».

В условиях динамично меняющейся международно-политической ситуации стратегии цифрового развития государств «Глобального Юга» характеризуются гибкостью и адаптивностью. Реагируя на американо-китайское соперничество, государства «Глобального Юга» различным образом модифицируют свои стратегии. Можно ожидать, что стратегии стран «Глобального Юга» будут корректироваться с учетом дальнейшей трансформации американо-китайских отношений.

Менее развитые в технологическом отношении страны «Глобального Юга», прежде всего государства Африки южнее Сахары, опасаются «цифровой колонизации» как со стороны американских, так и со стороны китайских корпораций. Эти страны

«Глобального Юга» заинтересованы в том, чтобы сохранять на своем внутреннем рынке присутствие и американских, и китайских корпораций, в том числе в целях получения от них новых технологий и конкурентных цен. Наиболее мощные страны «Глобального Юга» стремятся максимально диверсифицировать свои цифровые связи, разнообразие которых призвано в том числе способствовать хеджированию этими странами «Глобального Юга» политических и экономических рисков, а также решению таких задач, как усиление технологического потенциала национальных цифровых компаний, использование своих конкурентных преимуществ для привлечения зарубежных инвестиций в цифровой сегмент национальных экономик, а также активизация своего транспортно-логистического потенциала благодаря внедрению технологий Четвертой промышленной революции.

В условиях трансформации регионально-глобально-международно-политического пространства параллельная реализация странами «Глобального Юга» амбициозных программ цифрового развития указывает на то, что в перспективе вероятно усиление конкуренции между этими странами в цифровой сфере. Вместе с тем в настоящее время страны «Глобального Юга» стремятся создавать определенные условия для осуществления регионального и трансрегионального международного сотрудничества в области разработки и применения цифровых технологий, в том числе в целях укрепления своих позиций в Индо-Тихоокеанском регионе. Для решения этой задачи государства «Глобального Юга» предпринимают меры, направленные на формирование и развитие «гибких» международных партнерств с участием зарубежных государств и технологических компаний по линии «Юг — Север» и «Юг — Юг».

Поступила в редакцию / Received: 19.01.2022

Доработана после рецензирования / Revised: 06.03.2022

Принята к публикации / Accepted: 18.04.2022

Библиографический список

- Дегтерев Д. А., Рамич М. С., Пискунов Д. А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // Вестник международных организаций. 2021. Т. 16, № 3. С. 7—33. <https://doi.org/10.17323/1996-7845-2021-03-01>
- Дегтерев Д. А., Рамич М. С., Цвык А. В. США — КНР: «властный транзит» и контуры «конфликтной биполярности» // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2021. Т. 21, № 2. С. 210—231. <https://doi.org/10.22363/2313-0660-2021-21-2-210-231>

- Ефременко Д. В.* Формирование цифрового общества и геополитическая конкуренция // *Контуры глобальных трансформаций: политика, экономика, право*. 2020. Т. 13, № 2. С. 25—43. <https://doi.org/10.23932/2542-0240-2020-13-2-2>
- Кириченко И. В.* Индия: программа цифровизации как ключ к решению социальных проблем // *Азия и Африка сегодня*. 2021. № 7. С. 5—13. <https://doi.org/10.31857/S032150750014771-0>
- Коваль А. Г., Андрианова Е. К.* Перспективы развития цифровой экономики в Mercosur // *Латинская Америка*. 2020. № 3. С. 18—32. <https://doi.org/10.31857/S0044748X0008389-6>
- Кузнецов Д. А.* Соотношение трансрегионализации и глобализации в мировой политике // *Вестник МГИМО-Университета*. 2021. Т. 14, № 5. С. 65—80. <https://doi.org/10.24833/2071-8160-2021-5-80-65-80>
- Панцерев К. А.* Страны Африки южнее Сахары в цифровую эпоху: к вопросу обеспечения информационного суверенитета // *Азия и Африка сегодня*. 2019. № 10. С. 10—16. <https://doi.org/10.31857/S032150750006520-4>
- Перминов В. А.* Развитие умных городов в Индии // *Российский внешнеэкономический вестник*. 2020. № 8. С. 120—125.
- Расольцев С. В.* «Глобальный Юг»: происхождение и эволюция термина // *Мировое развитие: «Глобальный Юг» в полицентричном миропорядке*. Вып. 19 / под ред. К. Р. Воды, Т. А. Воротниковой, О. С. Кульковой, А. А. Невской, П. П. Тимофеева, А. А. Шинкаренко. Москва : ИМЭМО РАН, 2018. С. 5—11. <https://doi.org/10.20542/978-5-9535-0547-5>
- Ханна П.* Коннектография. Будущее глобальной цивилизации. Москва : Манн, Иванов и Фербер, 2019.
- Яковлев П. П.* Глобальный Юг: концептуальные подходы и социально-экономические процессы // *Контуры глобальных трансформаций: политика, экономика, право*. 2021. Т. 14, № 2. С. 6—27. <https://doi.org/10.23932/2542-0240-2021-14-2-1>
- Amadi L.* Globalization and the Changing Liberal International Order: A Review of the Literature // *Research in Globalization*. 2020. Vol. 2. P. 1—9. <https://doi.org/10.1016/j.resglo.2020.100015>
- Atkinson R. D.* A U.S. Grand Strategy for the Global Digital Economy // *Information Technology & Innovation Foundation*. 2021. P. 1—61. URL: <https://itif.org/publications/2021/01/19/us-grand-strategy-global-digital-economy> (accessed: 07.08.2021).
- Benyera E.* The Fourth Industrial Revolution and the Recolonization of Africa. The Coloniality of Data. London : Taylor & Francis, 2021. <https://doi.org/10.4324/9781003157731>
- Bogdanov K. V.* Flexible Coalitions: Origins and Prospects // *Russia in Global Affairs*. 2019. Vol. 17, no. 3. P. 132—150.
- Bueger C., Liebetrau T.* Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network // *Contemporary Security Policy*. 2021. Vol. 42, no. 3. P. 391—413. <https://doi.org/10.1080/13523260.2021.1907129>
- Haider S. A., Zeeshan M., Irshad M., Noman S. M., Arshad J., Shah S. M. A. et al.* The Inclusive Analysis of ICT Ethical Issues on Healthy Society: A Global Digital Divide Approach // *Procedia Computer Science*. 2021. Vol. 183. P. 801—806. <https://doi.org/10.1016/j.procs.2021.03.001>
- Iyer K. C., Nanyam V. P. S. N.* Technical Efficiency Analysis of Container Terminals in India // *The Asian Journal of Shipping and Logistics*. 2021. Vol. 37, no. 1. P. 61—72. <https://doi.org/10.1016/j.ajsl.2020.07.002>
- Kim H.* Globalization and Regulatory Change: The Interplay of Laws and Technologies in E-commerce in Southeast Asia // *Computer Law & Security Review*. 2019. Vol. 35, no. 5. P. 1—20. <https://doi.org/10.1016/j.clsr.2019.03.009>
- Kim M.-J., Lee H., Kwak J.* The Changing Patterns of China's International Standardization in ICT under Techno-nationalism: A Reflection through 5G Standardization // *International Journal of Information Management*. 2020. Vol. 54. P. 1—8. <https://doi.org/10.1016/j.ijinfomgt.2020.102145>
- Kong L., Woods O.* Scaling Smartness, (De)provincialising the City? The ASEAN Smart Cities Network and the Translational Politics of Technocratic Regionalism // *Cities*. 2021. Vol. 117. P. 1—8. <https://doi.org/10.1016/j.cities.2021.103326>
- Kulesza J., Weber R. H.* Protecting the Internet with International Law // *Computer Law & Security Review*. 2021. Vol. 40. P. 1—12. <https://doi.org/10.1016/j.clsr.2021.105531>
- Mansell R.* Adjusting to the Digital: Societal Outcomes and Consequences // *Research Policy*. 2021. Vol. 50, no. 9. P. 1—10. <https://doi.org/10.1016/j.respol.2021.104296>
- Muraviev A. D., Ahlawat D., Hughes L.* India's Security Dilemma: Engaging Big Powers while Retaining Strategic Autonomy // *International Politics*. 2021. P. 1—20. <https://doi.org/10.1057/s41311-021-00350-z>
- Nie M.* Asian Space Cooperation and Asia-Pacific Space Cooperation Organization: An Appraisal of Critical Legal Challenges in the Belt and Road Space Initiative Context // *Space Policy*. 2019. Vol. 47. P. 224—231. <https://doi.org/10.1016/j.spacepol.2019.01.008>

- Okano-Heijmans M., Vosse W. Promoting Open and Inclusive Connectivity: The Case for Digital Development Cooperation // *Research in Globalization*. 2021. Vol. 3. P. 1—10. <https://doi.org/10.1016/j.resglo.2021.100061>
- Potluri S. R., Sridhar V., Rao S. Effects of Data Localization on Digital Trade: An Agent-based Modeling Approach // *Telecommunications Policy*. 2020. Vol. 44, no. 9. P. 1—16. <https://doi.org/10.1016/j.telpol.2020.102022>
- Ross A., Banerjee S., Chowdhury A. Security in Smart Cities: A Brief Review of Digital Forensic Schemes for Biometric Data // *Pattern Recognition Letters*. 2020. Vol. 138. P. 346—354. <https://doi.org/10.1016/j.patrec.2020.07.009>
- Santra A., Mahato S., Mandal S., Dan S., Verma P., Banerjee P. et al. Augmentation of GNSS Utility by IRNSS/NavIC Constellation over the Indian Region // *Advances in Space Research*. 2019. Vol. 63, no. 9. P. 2995—3008. <https://doi.org/10.1016/j.asr.2018.04.020>
- Shattuck T. J. Stuck in the Middle: Taiwan's Semiconductor Industry, the U.S. — China Tech Fight, and Cross-Strait Stability // *Orbis*. 2021. Vol. 65, no. 1. P. 101—117. <https://doi.org/10.1016/j.orbis.2020.11.005>
- Trevisan C. The Risks to Latin America from the Breakdown of US — China Relations // *Asian Perspective*. 2021. Vol. 45, no. 1. P. 191—201. <https://doi.org/10.1353/apr.0.0012>
- Williams L. D. Concepts of Digital Economy and Industry 4.0 in Intelligent and Information Systems // *International Journal of Intelligent Networks*. 2021. Vol. 2. P. 122—129. <https://doi.org/10.1016/j.ijin.2021.09.002>
- Yan Y. Capacity Building in Regional Space Cooperation: Asia-Pacific Space Cooperation Organization // *Advances in Space Research*. 2021. Vol. 67, no. 1. P. 597—616. <https://doi.org/10.1016/j.asr.2020.10.022>
- Zhao B., Feng Y. Mapping the Development of China's Data Protection Law: Major Actors, Core Values, and Shifting Power Relations // *Computer Law & Security Review*. 2021. Vol. 40. P. 1—16. <https://doi.org/10.1016/j.clsr.2020.105498>

References

- Amadi, L. (2020). Globalization and the changing liberal international order: A review of the literature. *Research in Globalization*, 2, 1—9. <https://doi.org/10.1016/j.resglo.2020.100015>
- Atkinson, R. D. (2021). A U.S. grand strategy for the global digital economy. *Information Technology & Innovation Foundation*, 1—61. Retrieved from: <https://itif.org/publications/2021/01/19/us-grand-strategy-global-digital-economy>
- Benyera, E. (2021). *The Fourth industrial revolution and the recolonization of Africa. The coloniality of data*. London: Taylor & Francis. <https://doi.org/10.4324/9781003157731>
- Bogdanov, K. V. (2019). Flexible coalitions: Origins and prospects. *Russia in Global Affairs*, 17(3), 132—150. (In Russian).
- Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy*, 42(3), 391—413. <https://doi.org/10.1080/13523260.2021.1907129>
- Degterev, D. A., Ramich, M. S., & Tsyvyk, A. V. (2021). U.S. — China: “Power transition” and the outlines of “conflict bipolarity”. *Vestnik RUDN. International Relations*, 21(2), 210—231. <https://doi.org/10.22363/2313-0660-2021-21-2-210-231>
- Degterev, D. A., Ramich, M. S., & Piskunov, D. A. (2021). U.S. & China approaches to global internet governance: “New bipolarity” in terms of “the network society”. *International Organisations Research Journal*, 16(3), 7—33. <https://doi.org/10.17323/1996-7845-2021-03-01>
- Efremenko, D. V. (2020). Formation of digital society and geopolitical competition. *Outlines of Global Transformations: Politics, Economics, Law*, 13(2), 25—43. (In Russian). <https://doi.org/10.23932/2542-0240-2020-13-2-2>
- Haider, S. A., Zeeshan, M., Irshad, M., Noman, S. M., Arshad, J., & Shah, S. M. A., et al. (2021). The inclusive analysis of ICT ethical issues on healthy society: A global digital divide approach. *Procedia Computer Science*, 183, 801—806. <https://doi.org/10.1016/j.procs.2021.03.001>
- Iyer, K. C., & Nanyam, V. P. S. N. (2021). Technical efficiency analysis of container terminals in India. *The Asian Journal of Shipping and Logistics*, 37(1), 61—72. <https://doi.org/10.1016/j.ajsl.2020.07.002>
- Khanna, P. (2019). *Connectography: Mapping the future of global civilization*. Moscow: Mann, Ivanov i Ferber publ. (In Russian).
- Kim, H. (2019). Globalization and regulatory change: The interplay of laws and technologies in E-commerce in Southeast Asia. *Computer Law & Security Review*, 35(5), 1—20. <https://doi.org/10.1016/j.clsr.2019.03.009>
- Kim, M.-J., Lee, H., & Kwak, J. (2020). The changing patterns of China's international standardization in ICT under techno-nationalism: A reflection through 5G standardization. *International Journal of Information Management*, 54, 1—8. <https://doi.org/10.1016/j.ijinm.2020.102145>

- Kirichenko, I. V. (2021). India: Digitalization program as the key to social problems solving. *Asia and Africa Today*, (7), 5—13. (In Russian). <https://doi.org/10.31857/S032150750014771-0>
- Kong, L., & Woods, O. (2021). Scaling smartness, (de)provincialising the city? The ASEAN Smart Cities Network and the translational politics of technocratic regionalism. *Cities*, 117, 1—8. <https://doi.org/10.1016/j.cities.2021.103326>
- Koval, A. G., & Andrianova, E. K. (2020). Prospects of digital economic development in Mercosur. *Latinskaia Amerika*, (3), 18—32. (In Russian). <https://doi.org/10.31857/S0044748X0008389-6>
- Kulesza, J. & Weber, R. H. (2021). Protecting the Internet with international law. *Computer Law & Security Review*, 40, 1—12. <https://doi.org/10.1016/j.clsr.2021.105531>
- Kuznetsov, D. A. (2021). Transregionalization in the context of globalization, *MGIMO Review of International Relations*, 14(5), 65—80. (In Russian). <https://doi.org/10.24833/2071-8160-2021-5-80-65-80>
- Mansell, R. (2021). Adjusting to the digital: Societal outcomes and consequences. *Research Policy*, 50(9), 1—10. <https://doi.org/10.1016/j.respol.2021.104296>
- Muraviev, A. D., Ahlawat, D., & Hughes, L. (2021). India's security dilemma: Engaging big powers while retaining strategic autonomy. *International Politics*, 1—20. <https://doi.org/10.1057/s41311-021-00350-z>
- Nie, M. (2019). Asian space cooperation and Asia-Pacific space cooperation organization: An appraisal of critical legal challenges in the Belt and Road space initiative context. *Space Policy*, 47, 224—231. <https://doi.org/10.1016/j.spacepol.2019.01.008>
- Okano-Heijmans, M., & Vosse, W. (2021). Promoting open and inclusive connectivity: The case for digital development cooperation. *Research in Globalization*, 3, 1—10. <https://doi.org/10.1016/j.resglo.2021.100061>
- Pantserev, K. A. (2019). States of Sub-Saharan Africa at the digital age: To the problem of the ensuring of the information sovereignty. *Asia and Africa Today*, (10), 10—16. (In Russian). <https://doi.org/10.31857/S032150750006520-4>
- Perminov, V. A. (2020). Smart city development in India. *Russian Foreign Economic Journal*, (8), 120—125. (In Russian).
- Potluri, S. R., Sridhar, V., & Rao, S. (2020). Effects of data localization on digital trade: An agent-based modeling approach. *Telecommunications Policy*, 44(9), 1—16. <https://doi.org/10.1016/j.telpol.2020.102022>
- Rastoltsev, S. V. (2018). “Global South”: The origin and evolution of the term. In K. R. Voda, T. A. Vorotnikova, O. S. Kulkova, A. A. Nevskaya, P. P. Timofeev & A. A. Shinkarenko (Eds.), *Global development: Global South in the polycentric world* (Iss. 19, pp. 5—11). Moscow: IMEMO publ. (In Russian). <https://doi.org/10.20542/978-5-9535-0547-5>
- Ross, A., Banerjee, S., & Chowdhury, A. (2020). Security in smart cities: A brief review of digital forensic schemes for biometric data. *Pattern Recognition Letters*, 138, 346—354. <https://doi.org/10.1016/j.patrec.2020.07.009>
- Santra, A., Mahato, S., Mandal, S., Dan, S., Verma, P., & Banerjee, P., et al. (2019). Augmentation of GNSS utility by IRNSS/NavIC constellation over the Indian region. *Advances in Space Research*, 63(9), 2995—3008. <https://doi.org/10.1016/j.asr.2018.04.020>
- Shattuck, T. J. (2021). Stuck in the middle: Taiwan's semiconductor industry, the U.S. — China tech fight, and cross-strait stability. *Orbis*, 65(1), 101—117. <https://doi.org/10.1016/j.orbis.2020.11.005>
- Trevisan, C. (2021). The risks to Latin America from the breakdown of US — China relations. *Asian Perspective*, 45(1), 191—201. <https://doi.org/10.1353/apr.0.0012>
- Williams, L. D. (2021). Concepts of digital economy and industry 4.0 in intelligent and information systems. *International Journal of Intelligent Networks*, 2, 122—129. <https://doi.org/10.1016/j.ijin.2021.09.002>
- Yakovlev, P. P. (2021). Global South: Conceptual approaches and socioeconomic processes. *Outlines of Global Transformations: Politics, Economics, Law*, 14(2), 6—27. (In Russian). <https://doi.org/10.23932/2542-0240-2021-14-2-1>
- Yan, Y. (2021). Capacity building in regional space cooperation: Asia-Pacific space cooperation organization. *Advances in Space Research*, 67(1), 597—616. <https://doi.org/10.1016/j.asr.2020.10.022>
- Zhao, B., & Feng, Y. (2021). Mapping the development of China's data protection law: Major actors, core values, and shifting power relations. *Computer Law & Security Review*, 40, 1—16. <https://doi.org/10.1016/j.clsr.2020.105498>

Сведения об авторе: Столетов Олег Владимирович — кандидат политических наук, доцент кафедры международных отношений и интеграционных процессов факультета политологии, МГУ имени М.В. Ломоносова; ORCID: 0000-0003-0479-7865; e-mail: oleg-stoletov1@yandex.ru

About the author: Stoletov Oleg Vladimirovich — PhD in Political Sciences, Assistant Professor, Department of International Relations and Integration Processes, The Faculty of Political Science, Moscow State University; ORCID: 0000-0003-0479-7865; e-mail: oleg-stoletov1@yandex.ru



DOI: 10.22363/2313-0660-2022-22-2-238-255

Научная статья / Research article

Секьюритизация информационного пространства: от конструирования норм до создания правовых режимов

М.С. Рамич  , Д.А. Пискунов 

Российский университет дружбы народов, Москва, Российская Федерация

ramich-ms@rudn.ru

Аннотация. С развитием информационно-коммуникационных технологий (ИКТ) сеть Интернет стала приобретать большее значение с точки зрения национальной безопасности, экономического развития и мирового лидерства. Конфликты и спорные вопросы, возникающие в информационном пространстве, требуют согласования норм и выработки инструментов правового регулирования. Авторы статьи рассматривают процесс конструирования норм в информационном пространстве с точки зрения теории «сетевого общества» М. Кастельса и теории секьюритизации. По мнению М. Кастельса, в «сетевом обществе» произошла смена ключевых вызовов и угроз, а управление им стало осуществляться за счет инструментов контроля над информацией и формирования фреймов. Вместе с тем авторы, анализируя развитие сети Интернет с точки зрения концепции секьюритизации, приходят к выводу, что информационное пространство стало полноценным политическим пространством с центральным положением «цифрового суверенитета» и информационной безопасности. В статье впервые предлагается комплексная периодизация процесса трансформации международных отношений в информационном пространстве. Возникновение в информационном пространстве точек напряженности, которые несут экономические и политические риски, побуждает государственных акторов к формированию предварительного регулирования и согласованию норм поведения в информационном пространстве. Такой процесс конструирования предварительного регулирования был начат под эгидой ООН в рамках двух механизмов, созданных США и Россией. Эти механизмы стали площадкой для продвижения концепций регулирования и создания правовых режимов. В заключении авторы анализируют иерархию акторов в глобальном управлении информационным пространством с целью оценить влияние акторов на создание правовых режимов. Основными критериями оценки выступают способность влиять на глобальные цепочки производства высокотехнологичных товаров, проводить наступательные и оборонительные кибероперации и влиять на формирование международно-правовых режимов. Среди таких акторов авторы выделяют две группы: rule maker, способных воздействовать на глобальное информационное пространство и конструировать правовые режимы, и rule taker, которые выступают объектом конкуренции держав в информационном пространстве.

Ключевые слова: сетевое общество, информационное пространство, секьюритизация, США, КНР, Россия

Для цитирования: Рамич М. С., Пискунов Д. А. Секьюритизация информационного пространства: от конструирования норм до создания правовых режимов // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 238—255. <https://doi.org/10.22363/2313-0660-2022-22-2-238-255>

© Рамич М.С., Пискунов Д.А., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

The Securitization of Cyberspace: From Rulemaking to Establishing Legal Regimes

Mirzet S. Ramich  , Danil A. Piskunov 

Peoples' Friendship University of Russia (RUDN University), Moscow, Russian Federation

 ramich-ms@rudn.ru

Abstract. With the development of information and communication technologies (ICTs), the Internet has become increasingly important in terms of national security, economic development, and global leadership. Apparently, conflicts and contentious issues in cyberspace requires creating rules and development of regulation. The authors examine the process of making up rules in cyberspace from the perspective of M. Castells' network society theory and B. Buzan' securitization theory. According to M. Castells, key challenges have gradually altered in the network society and power relations and social management are based on the control of communication and information which embraces a network society. Furthermore, the authors investigate the development of the Internet in the context of securitization theory. It is stressed that cyberspace has become a full-fledged political space with the central position of digital sovereignty and information security. The article for the first time proposes a comprehensive periodization of international relations' transformation in cyberspace. Afterwards, the authors consider the appearance of tensions between actors in cyber space, which include political and economic threats. It encourages state actors to establish a preliminary regulation and to agree on norms regulating state behavior in cyberspace. These mechanisms have become a venue for promoting different concepts of cyber law and establishing legal regimes. In conclusion the authors analyze the hierarchy of actors in global Internet governance to assess the actors' influence on the establishment of legal regimes in cyberspace. The main assessment criteria are as follows: ability to influence global production chains of high-tech goods, ability to conduct offensive and defensive cyber operations, and influence on the formation of international legal regimes. The authors divide actors into two major groups — rule-markers capable of influencing the global information space and constructing legal regimes, and rule-takers that are an object of great powers competition in cyberspace.

Key words: network society, cyberspace, securitization, US, China, Russia

For citation: Ramich, M. S., & Piskunov, D. A. (2022). The securitization of cyberspace: From rulemaking to establishing legal regimes. *Vestnik RUDN. International Relations*, 22(2), 238—255. <https://doi.org/10.22363/2313-0660-2022-22-2-238-255>

Введение

Развитие и внедрение информационно-коммуникационных технологий (ИКТ) в конце XX — начале XXI в. привело к повышению уровня цифровизации общества и экономики государств. В таких условиях с точки зрения национальной безопасности государства на первый план выходит информационная безопасность, которая подразумевает обеспечение функционирования инфраструктурных объектов, ограничение иностранного влияния и управление внутренним сегментом сети Интернет. Критическая важность информационной безопасности обусловлена, во-первых, отсутствием всеобъемлющего правового регулирования отношений между

государствами в киберпространстве, во-вторых, присутствием негосударственных акторов в сети Интернет, влияющих на информационную безопасность государств и, в-третьих, ролью информационной безопасности в процессах социального управления обществом.

В сети Интернет возникают точки напряженности и конфликты, которые подталкивают государства к выработке норм и правил взаимодействия в киберпространстве. Такие конфликты свидетельствуют о критической важности управления информационным пространством и обеспечения безопасности национальных объектов инфраструктуры. Этот факт усиливается тем, что в постбиполярный период фактор ядерного оружия и жестко-силового противостояния становится

менее актуальным¹. Это ведет к формированию предпосылок к выработке правил и норм ответственного поведения в информационном пространстве для государственных акторов.

С точки зрения регулирования киберпространства можно выделить два подхода — концепцию Запада (США + ЕС) и концепцию развивающихся стран (Китай + Россия) (Международная информационная безопасность: теория и практика, 2019; Зиновьева, 2019b). В них сформированы принципы в отношении таких ключевых вопросов, как информационная безопасность, развитие сети Интернет, глобальное управление киберпространством, администрирование внутренней сети Интернет и т. д. (Дегтерев, Рамич, Пискунов, 2021, с. 9). Конкуренция двух концепций обусловлена не только преимуществами с точки зрения национальной безопасности, но и усиливающимся противостоянием США и КНР на мировой арене (Данилин, 2020b; Дегтерев, Рамич, Цвык, 2021, с. 220).

Ключевым аспектом американо-китайской конфронтации выступает именно технологическая сфера, где обе стороны продвигают свои технологические экосистемы, начиная от концепций управления Интернетом и заканчивая технологическими сервисами и передовыми разработками (Данилин, 2020a; Xingdong & Du, 2019, p. 47). Технологическая конкуренция США и КНР важна ввиду того, что сегодня социальные сети и другие сервисы оказывают большое влияние на распространение социальных ценностей, идей и норм, которые формируют основу социального управления и создание образа восприятия государства (Castells, 2013). С точки зрения информационного влияния США и КНР конкурируют за глобальное распространение социальных приложений (TikTok, WeChat, Facebook², Google и др.)

¹ Lewis J. A. Technological Competition and China // Center for Strategic and International Studies. November 30, 2018. URL: <https://www.csis.org/analysis/technological-competition-and-china> (accessed: 26.02.2022). См. также: (Дегтерев, Рамич, Пискунов, 2021; Zhao, 2021, p. 3).

² 21.03.2022 г. Тверской районный суд г. Москвы удовлетворил иск Генпрокуратуры РФ и признал деятельность соцсетей Instagram и Facebook,

своих технологических корпораций (Данилин, 2020b).

Развитие сети Интернет и повсеместное внедрение ИКТ привело к оформлению «сетевого общества», в котором власть конструируется посредством контроля над коммуникацией в сети (Castells, 2011). В контексте теории «сетевого общества» М. Кастельса релевантным становится рассмотрение власти в формирующемся глобальном сетевом обществе, в котором власть того или иного актора будет конструироваться за счет установленных норм и правил поведения в киберпространстве.

Подходящим примером формирования правил поведения выступает регулирование в сфере ядерного оружия (Nye, 2011, p. 18). Дж. Най проводит сравнительный анализ конструирования норм и правил в сфере ядерного оружия и в киберпространстве (Nye, 2011, p. 22). По мнению американского исследователя, опыт конструирования правил поведения в ядерной сфере применим к информационному пространству ввиду того, что сеть Интернет и информационная безопасность выходят на первый план для государств с высоким уровнем цифровизации экономики и использования ИКТ на инфраструктурных объектах военного и гражданского назначения (Nye, 2016, p. 46).

В данной работе используется методологический инструментарий, в основе которого лежат теория «сетевого общества» и теория секьюритизации (раздел I), которые позволяют комплексно исследовать вопрос секьюритизации информационного пространства и предложить авторскую периодизацию этого процесса в зависимости от характера угроз и межгосударственного взаимодействия (раздел II). Проблемы отсутствия регулирования в информационном пространстве были показаны на примере точек напряженности (раздел III), после чего дается обзор процесса предрегулирования в данной сфере и представлены основные проекты международно-правовых режимов (раздел IV). В завершающей части статьи авторы предлагают свой взгляд на иерархию системы глобального

принадлежащих Meta, экстремистской, запретив их работу в России.

управления в информационном пространстве (раздел V). В заключении резюмируются основные положения по каждому из исследованных аспектов и даются прогнозы относительно будущего системы глобального управления в информационном пространстве.

I. Методология

Выбор методологического инструментария обуславливается комплексным характером проблем в информационном пространстве, для анализа которых необходимо использовать междисциплинарный подход. В данной статье основу методологии составляют теория секьюритизации и теория «сетевого общества».

В XXI в. информационное пространство стало полноценным политическим пространством, на которое частично сместился фокус во всех сферах международных отношений, начиная от социально-экономического взаимодействия и заканчивая вопросами международной безопасности. Трансформацию характера угроз и межгосударственного взаимодействия в информационном пространстве можно проследить через призму теории секьюритизации, которая была предложена представителями Копенгагенской школы (Buzan, 1983; Buzan & Wæver, 2003; Buzan & Hansen, 2009; Hansen & Nissenbaum, 2009). Данная теория обеспечивает устойчивую методологическую основу для исследования вопросов безопасности в информационном пространстве, так как проблемы в цифровом домене не существуют в вакууме и чаще всего носят глобальный характер, оказывая влияние на международную систему без привязки к государственным границам (Hjalmarsson, 2013, p. 4). В данной статье авторы предлагают сопоставить трансформацию проблем безопасности и международного регулирования информационного пространства, сравнив характер угроз, основных акторов и международные правовые режимы, чтобы проследить хронологию секьюритизации информационного пространства начиная с момента создания Интернета (табл. 1). Технологическое развитие и увеличение пользователей ИКТ создало прецедент для перехода угроз из физического домена в цифровой, где система

взаимодействия между акторами представляется анархичной и не контролируется общепринятыми нормативно-правовыми режимами.

За счет специфики информационного пространства изменился и характер так называемых «узких мест», или точек напряженности, в информационном пространстве. Если изначально наиболее уязвимыми местами цифрового домена считалась критическая инфраструктура — корневые серверы и т. д., то вместе с эволюцией характера взаимодействия и угроз точки напряженности стали «виртуальными».

В социальной сфере также происходили беспрецедентные трансформации. Менялся характер поведения пользователей, а государства, в свою очередь, адаптировали свою политику к новым реалиям. Общество стало переходить на коммуникацию посредством устройств, подключенных к глобальной сети Интернет. На данный момент более 4,8 млрд человек используют Интернет, и большая часть (90 %) выходят в Интернет с мобильных устройств³. Вместе с тем стали происходить изменения в природе власти в обществе. Традиционная власть, как правило, применяющая методы наказания и запугивания, стала трансформироваться в сетевую власть, которая реализуется посредством создания (*framing*) идей и контроля над коммуникацией (Castells, 2011; 2013). Теория «сетевого общества» позволяет рассматривать власть государства в сетевом обществе как критический аспект национальной безопасности, так как иностранное влияние на общество извне способно подорвать установленные идеи и фреймы общества и впоследствии получить механизмы управления обществом.

По М. Кастельсу, властные отношения в сетевом обществе являются основой, а созданные в нем институты и нормы необходимы для продвижения интересов и ценностей этой власти (Castells, 2011). Главной характеристикой такого общества является формирование властных отношений, в которых властную позицию занимают институты управления сетевым обществом, в том числе медиа-

³ Digital Around the World // DataReportal. URL: <https://datareportal.com/global-digital-overview> (accessed: 08.01.2022).

компании, технологические компании и политические институты, осуществляющие глобальное управление и надзор.

Будучи новым политическим пространством, информационное пространство играет важную роль не только в рамках вопросов влияния и управления в сетевом обществе, но и в контексте современных международных экономических и политических отношений. Такие отношения, формируемые между государственными и негосударственными акторами, требуют правил поведения и норм, однако на данный момент отсутствует полноценное регулирование взаимоотношений в этой сфере. Релевантным примером конструирования норм поведения является выработка правил поведения в сфере ядерного оружия, описанная Дж. Наем (Nye, 2011).

II. Секьюритизация информационного пространства

Процесс секьюритизации в информационном пространстве можно разделить на несколько этапов в зависимости от основных акторов, характера угроз и международно-правового контекста. Сеть Интернет, которая стала основным полем обмена информацией в XXI в., изначально использовалась для решения узкоспециализированных задач. Основным направлением работы на первых этапах была научная и коммуникационная составляющая, поэтому новые угрозы безопасности на этих этапах не формировались. Аналогичным образом до начала 2000-х гг. нельзя было говорить о глобальном характере развития цифрового пространства.

В контексте сравнения с процессом развития ядерных технологий можно проследить четкую параллель. До начала Второй мировой войны их развитие в целом ограничивалось научной и энергетической сферами. Однако мировая война и открытие контролируемых термоядерных реакций стали теми причинами, которые способствовали распространению ядерных технологий на военную сферу. Таким образом, ядерное оружие и угроза тотальной ядерной войны стали основными вопросами в сфере международной безопасности во время холодной войны и остаются таковыми и в настоящее время.

Если говорить о киберпространстве и международной информационной безопасности, то разработка международных норм и правил поведения отставала от процесса развития ИКТ, что послужило причиной возникновения целого ряда новых вызовов и угроз в цифровом домене. В киберпространстве решающую роль играет технологическое развитие, которое также оказало значительное влияние на развитие межгосударственного взаимодействия в рамках морского и воздушного пространств (Ratray, 2009).

На политическом уровне киберпространство было включено в систему обеспечения национальной и международной безопасности в начале 2000-х гг. Как и в случае с другими новыми вызовами и угрозами, международное внимание к кибербезопасности было связано с ускорением процесса глобализации. После терактов 11 сентября 2001 г. многие государства задумались о том, какие вызовы могут происходить из мировой сети и какие возможности она может предоставить, принимая во внимание, что цифровой домен напрямую не контролируется национальными институтами (Stevens, 2012, p. 164).

Именно в 2001 г. был принят первый международный документ, который регулировал вопросы кибербезопасности, — Конвенция Совета Европы о киберпреступности (*The Budapest Convention on Cybercrime, the Budapest Convention*)⁴. В 2003 г. в рамках ООН была подписана Декларация принципов построения информационного общества⁵, а в 2005 г. были приняты Тунисское обязательство⁶ и Тунисская повестка по информационному обществу⁷. Подписание этих

⁴ Budapest Convention on Cybercrime // Council of Europe. November 23, 2001. URL: <https://rm.coe.int/1680081561> (accessed: 08.01.2022).

⁵ Declaration of Principles “Building the Information Society: A Global Challenge in the New Millennium” // International Telecommunication Union. December 12, 2003. URL: <https://digitallibrary.un.org/record/533621/files/S03-WSIS-DOC-0004%21%21PDF-E.pdf> (accessed: 08.01.2022).

⁶ Tunis Commitment (WSIS-05/TUNIS/DOC/7-E) // International Telecommunication Union. November 18, 2005. URL: <https://www.itu.int/net/wsisis/docs2/tunis/off/7.html> (accessed: 08.01.2022).

⁷ Tunis Agenda for the Information society (WSIS-05/TUNIS/DOC/6(Rev.1)-E) // International

документов стало предпосылкой к созданию в 2006 г. Всемирного форума по управлению Интернетом⁸.

Данный этап стал важной вехой в процессе признания международных вопросов, связанных с обеспечением международной безопасности в информационном пространстве, так как были даны определения новым вызовам и угрозам, созданы новые форматы взаимодействия. Однако в рамках этого процесса не было полноценного охвата всех вопросов, связанных с регулированием Интернета, что было обусловлено восприятием глобальной сети исключительно как средства связи. Ситуация изменилась к началу 2010-х гг., когда Интернет и информационное пространство стали системообразующим элементом научно-технического и экономического развития большинства стран мира.

В 2010-е гг. увеличилось количество пользователей информационных технологий, для государств это означало необходимость регулирования нового политического пространства. Именно в это время большой охват начали получать протоколы связи 4-го поколения (4G)⁹, которые выступили драйвером развития мобильного Интернета и значительно увеличили доступность сетевых ресурсов. Угрозы в информационном пространстве одновременно были и «реальными», и «виртуальными» — это угрозы для физических элементов сети или критической инфраструктуры и угрозы, которые исходят непосредственно из сетевого пространства и среди которых — широкий спектр международных угроз, начиная от нарушения авторских прав до ведения незаконной политической деятельности (Deibert & Rohozinski, 2010, pp. 29—30).

Значительно выросло число зафиксированных межгосударственных киберинцидентов.

Telecommunication Union. November 18, 2005. URL: <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html> (accessed: 08.01.2022).

⁸ Управление через Интернет // Отдел государственных учреждений и цифрового правительства Департамента ООН по экономическим и социальным вопросам. URL: <https://publicadministration.un.org/ru/internetgovernance> (дата обращения: 08.01.2022).

⁹ В 2009 г. в Стокгольме и Осло были запущены первые коммерческие сети 4G. Далее на новые протоколы связи стали переходить и другие страны. В некоторых странах процесс перехода до сих пор не завершен.

Если за 2003—2009 гг. было зафиксировано всего 66 подобных инцидентов, то только за 2017 г. их число превысило 71 случай, а в 2018 и 2019 гг. составило 114 и 116 соответственно¹⁰. Помимо этого, информационно-коммуникационные технологии стали одним из основных факторов в событиях «арабской весны»¹¹ и в целом использовались для организации «цветных революций» (Манойло, 2014). Для государств, которые не обладали достаточным уровнем технологий и опытом противодействия новым видам угроз, риски, исходящие из информационного пространства, стали одной из серьезных угроз для национального суверенитета и стабильности. В это же время технологически развитые государства получили возможность использовать новые инструменты для достижения своих внешнеполитических целей.

В 2015 г. был утвержден доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, который объединил достижения работы трех групп экспертов в 2010, 2013 и 2015 гг. Данный документ обобщил понятия угроз в информационном пространстве и предложил нормы и правила поведения для государств¹². В 2013 г. Центр передового опыта совместной киберзащиты НАТО опубликовал Таллинское руководство по международному праву, применимому к кибернетическим войнам. В 2017 г. вышло второе издание, и в настоящее время идет работа над третьей версией. Отличительной особенностью документа стало то, что там рассматривалась возможность физического военного ответа на

¹⁰ Significant Cyber Incidents // Center of Strategic International Studies. URL: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents> (accessed: 01.02.2022).

¹¹ Eriksson M., Franke U., Granåsen M., Lindahl D. Social Media and ICT during the Arab Spring // FOI Report. 2013. P. 46. URL: <https://www.foi.se/rest-api/report/FOI-R--3702--SE> (accessed: 08.01.2022).

¹² Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174 // General Assembly of the United Nations. July 22, 2015. URL: <https://namib.online/wp-content/uploads/2020/04/Report-of-the-UN-Group-of-Governmental-Experts-on-Developments-in-the-Field-of-Information-of-22-July-2015.pdf> (accessed: 08.01.2022).

кибератаки¹³. Во второй версии была дана классификация кибератак, которые можно считать нарушением суверенитета страны (повлекшие за собой человеческие жертвы или физический урон)¹⁴. Вместе с принятием таких документов был запущен процесс создания международных нормативно-правовых режимов для регулирования поведения государств в информационном пространстве.

В процессе секьюритизации информационного пространства страны начали наращивать свои наступательные и оборонительные потенциалы, что фактически привело к «дилемме безопасности» в киберпространстве. В таких условиях сильные государства могут одновременно устанавливая удобные для них правила и сами их нарушать, проводя политику двойных стандартов, в это же время более слабые государства не могут ничего им противопоставить (Buchanan, 2017, pp. 192—193). Таким образом, технологически более развитые государства получили большее влияние в киберпространстве, так как начали реализовывать свои проекты в новом политическом пространстве раньше других.

В данных условиях особенно актуальной стала проблема атрибуции враждебных действий в информационном пространстве. В большинстве своем речь идет о кибератаках и киберпреступлениях, которые совершаются хакерскими группами, принадлежность которых к тому или иному государству практически невозможно определить. Несмотря на появление специализированных учреждений по предупреждению инцидентов в информационном пространстве, вопрос атрибуции сохраняет комплексный характер (Зиновьева, 2019а, с. 58). Ряд стран прилагали усилия для налаживания обмена разведанными и компьютерной информацией о вредоносной активности в информационном пространстве на их территории. Так, в Европейском союзе вопрос атрибуции регламентирован в рамках

Будапештской конвенции 2001 г., к которой также присоединились США, Канада, Япония, Австралия и др.¹⁵ Вместе с тем Россия и страны Шанхайской организации сотрудничества (ШОС) также применяют практику обмена разведанными при координации соответствующих ведомств¹⁶. В соглашении между Россией и Китаем об обеспечении международной информационной безопасности также предусмотрен пункт обмена информацией, разведанными о вредоносной активности в информационном пространстве¹⁷. Тем самым приобретает опыт работы с установлением авторства атаки в информационном пространстве.

На частном уровне ведущие международные ИТ-компании по разработке систем защиты от вирусов, хакерских атак и иных киберугроз в атрибуции кибератаки используют метод анализа кода, или так называемого «почерка хакеров»¹⁸. Например, атрибуция атак в «Лаборатории Касперского» — это процесс сопоставления новых результатов инцидентов с накопленным опытом. Международная компания по информационной безопасности с целью успешной атрибуции атак создала базу данных *Kaspersky Threat Attribution Engine*, которая проводит анализ вредоносных программ и сопоставляет их с ранее сохраненной информацией¹⁹.

¹⁵ The Budapest Convention and its Protocols // Council of Europe. URL: <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (accessed: 01.02.2022).

¹⁶ Документы // Шанхайская организация сотрудничества. URL: <http://rus.sectsc.org/politics/> (дата обращения: 01.02.2022).

¹⁷ Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности // Официальный интернет-портал правовой информации. 08.05.2015. URL: <http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1> (дата обращения: 01.02.2022).

¹⁸ Оманд Д. Атрибуция кибератаки является политическим решением, это не судебный процесс // Ядерный Контроль. 2017. № 4 (486). URL: <http://www.pircenter.org/articles/2099-atribuciya-kiberataki-yavlyaetsya-politicheskim-resheniem-eto-nesudebnyj-process> (дата обращения: 01.02.2022).

¹⁹ Kaspersky Threat Attribution Engine // Kaspersky. URL: https://media.kaspersky.com/ru/business-security/enterprise/Kaspersky_Threat_Attribution_Engine_Product_Datasheet-ru.pdf (дата обращения: 01.02.2022).

¹³ Tallinn Manual on the International Law Applicable to Cyber Warfare / ed. by M. N. Schmitt. Cambridge; New York : Cambridge University Press, 2013. <https://doi.org/10.1017/CBO9781139169288>

¹⁴ Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by M. N. Schmitt. Cambridge : Cambridge University Press, 2017. <https://doi.org/10.1017/9781316822524>

Таблица 1

Хронология процесса секьюритизации информационного пространства в 1970—2020-е гг.

Компонент/ Период	1970-е - 2000-е Интернет ради науки	2000-е Формирование цифро- вого домена	2010-е Секьюритизация кибер- пространства	2020 - н.в. Переход к метавселен- ным
Стандарт связи	2G	3G	4G	5G
Актеры	Отдельные государственные и частные структуры	Государства, негосударственные акторы, международные организации	Государства, негосударственные акторы, международные организации	Государства, негосударственные акторы, международные организации
Масштаб угроз	Локальный характер угроз	Локальный характер угроз	Международный характер угроз	Международный характер угроз
Характер угроз	Промышленный шпионаж, физическое воздействие на критическую инфраструктуру	Основа теневой экономики, угроза физической инфраструктуре	Появление нового типа вызовов и угроз безопасности, межгосударственные кибератаки	Преобладание угроз, исходящих из информационного пространства (виртуальных), над физическими угрозами (реальными)
Режимы	—	Формирование базовых международно-правовых режимов, международное сотрудничество в сфере обеспечения кибербезопасности	Борьба между различными подходами к международно-правовому регулированию информационного пространства	Формирование глобальных цифровых экосистем, увеличение цифрового разрыва, борьба за лидерство в технологической сфере

Источник: составлено авторами.

В рамках следующего этапа развития информационного пространства большее внимание стало уделяться созданию цифровых экосистем, которые предназначены для максимальной концентрации пользователей вокруг группы связанных приложений. Для обработки больших объемов данных потребовались протоколы связи с более высокой скоростью, поэтому начался ускоренный переход на сети 5G. Примером цифровой экосистемы, применяемой как на государственном, так и на частном уровне, является Microsoft 365. Необходимо учитывать тот факт, что данные пользователей хранятся и обрабатываются на серверах компании поставщика цифровых услуг, что создает потенциальные уязвимости для сохранности секретной информации и персональных данных. На 2021 г. большую часть серверов для облачных технологий предоставляют следующие компании: Amazon (США) — 33 %, Microsoft (США) — 21 %, Google (США) — 10 %, Alibaba (КНР) — 6 %, IBM (США) — 4 %, Salesforce (США) — 3 %, Tencent (КНР) — 3 % и Oracle (США) — 2 %²⁰.

²⁰ As Quarterly Cloud Spending Jumps to Over \$50B, Microsoft Looms Larger in Amazon's Rear Mirror //

Данная статистика наглядно иллюстрирует, что большую часть рынка облачных технологий контролируют компании из США, единственными конкурентами которых являются китайские компании, обеспечивающие работу облачных сервисов в Китае. О конкуренции на глобальном рынке на данный момент не может быть и речи. В странах, которые придерживаются принципов цифрового суверенитета, на законодательном уровне ограничивается трансграничная передача персональных данных и информации. Из-за специфики информационного пространства цифровой суверенитет в политическом понимании приведет к технологической изоляции страны. Таким образом, в информационном пространстве можно либо обеспечить суверенитет в пределах политических границ, либо добиться глобальной совместимости Интернета, которая будет означать взаимозависимость (Mueller, 2020, p. 798).

К началу 2020-х гг. в информационное пространство стало полноценным политическим

Synergy Research Group. February 3, 2022. URL: <https://www.srgresearch.com/articles/as-quarterly-cloud-spending-jumps-to-over-50b-microsoft-looms-larger-in-amazons-rear-mirror> (accessed: 26.02.2022).

пространством, которое занимает центральное место в процессах международного социально-экономического и технологического развития. К началу четвертого этапа стала особенно очевидной проблема цифрового суверенитета, который не может полностью соответствовать политическим границам государства. В это же время страны разделились на несколько объединений, которые выступают за различные формы регулирования межгосударственных отношений в информационном пространстве. США и развитые страны выступают за модель мультитейкхолдеризма в управлении цифровым доменом, в то время как Россия, Китай и развивающиеся страны выступают за многосторонний подход (Дегтерев, Рамич, Пискунов, 2021). Однако помимо государственных инициатив популяризация технологий блокчейн позволяет говорить о создании автономных децентрализованных систем вне государственного контроля²¹.

III. Потенциальные точки напряженности

Возникающие в информационном пространстве вызовы и угрозы привели к тому, что сфера ИКТ стала рассматриваться в качестве одной из основных сфер национальной безопасности (Hansen & Nissenbaum, 2009). К таким угрозам можно отнести нарушение функционирования объектов критической инфраструктуры, внешнее влияние во внутреннем информационном пространстве и т. д.

Авторы рассматривают точки напряженности в информационном пространстве и анализируют возможные сферы совпадения интересов и конструирования правил поведения в сети Интернет. По аналогии с ядерной сферой государственные акторы начали согласовывать негласные правила и нормы в сфере ядерного оружия с целью минимизировать риски его распространения, эскалации конфликта и т. д. (Nye, 2011). Основой для согласования первичных негласных норм в

²¹ Weyl G., Ohlhaber P., Buterin V. Decentralized Society: Finding Web3's Soul // Social Science Research Network. May 11, 2022. URL: <https://ssrn.com/abstract=4105763> (accessed: 26.05.2022).

ядерной сфере стал опыт конфликтов и кризисов с возможным использованием ядерного оружия. Конфликты в информационном пространстве с использованием вредоносного программного обеспечения (ПО) могут привести к «Карибскому кризису 2.0», который станет общей проблемой ведущих стран (Международная информационная безопасность..., 2021). Такая проблема станет стимулом для создания регулирования в информационном пространстве, так как ее решение требует совместных действий и взаимных обязательств по соблюдению норм.

С учетом специфики информационного пространства безопасность может быть разделена на два измерения: материальные риски для критической инфраструктуры, протоколов и оборудования и риски, возникающие в информационном пространстве без физического ущерба (Deibert & Rohozinski, 2010). В данном разделе будут рассмотрены конфликты и точки напряженности между акторами в ряде сфер, затрагивающих информационную безопасность: критическая инфраструктура, внешнее влияние и социальные приложения, технологическая безопасность и устойчивость цепочек поставок, а также суверенное управление внутренним сегментом сети Интернет.

С точки зрения рисков для физической инфраструктуры, находящейся под юрисдикцией государства, следует упомянуть кейс атаки на трубопровод Colonial Pipeline и JBS Foods, вследствие которой снабжение газом Восточного побережья США было приостановлено на пять дней, а пищевая компания JBS Foods вынуждена была приостановить работу заводов²². В результате нарушения функционирования инфраструктурных объектов администрация Дж. Байдена выпустила меморандум о защите критической инфраструктуры²³. Подобные атаки были произведе-

²² JBS and Colonial Pipeline Hacks Highlight How Large Food and Energy Companies Have Become Prime Targets // South China Morning Post. June 4, 2021. URL: <https://www.scmp.com/tech/tech-trends/article/3135990/jbs-and-colonial-pipeline-hacks-highlight-how-large-food-and> (accessed: 08.01.2021).

²³ Fact Sheet: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure // The White House. July 28, 2021. URL: <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet->

дены в 2019 г. и на российские энергетические системы. Авторство атак приписывают США²⁴. Для обоих государств защита критической инфраструктуры отвечает задачам национальной безопасности. В 2013 г. США выделили 16 секторов и признали, что атаки на объекты критической инфраструктуры подрывают национальную безопасность, а также воздействуют на экономическую и социально-гуманитарную безопасность²⁵. Россия в 2017 г. также приняла закон о безопасности критической информационной инфраструктуры²⁶.

С точки зрения законодательной системы КНР в сфере кибербезопасности следует отметить ряд документов, которые транслируют подходы внутреннего регулирования КНР на уровень глобального управления. В первую очередь необходимо выделить Закон о безопасности сети Интернет (в российской литературе именуется законом о кибербезопасности)²⁷. Законодательный акт, принятый в 2017 г., закрепил понятие цифрового суверенитета (网络空间主权) и требования к сетевым операторам хранить персональные данные граждан на территории КНР. В дополнение к этому в Законе была определена

система защиты критической инфраструктуры КНР. В 2021 г. Госсовет КНР опубликовал сразу ряд документов, конкретизирующих внутреннюю политику КНР в сфере кибербезопасности: Расширенное положение о защите критической инфраструктуры²⁸, Закон о безопасности данных²⁹ и Закон о защите персональных данных³⁰.

Кроме того, следует отметить напряженность между США и Китаем в сфере развития сетей 5G. На основе анализа указанных правовых документов можно сделать вывод, что КНР с целью обеспечения национальной безопасности принимает меры по локализации данных, созданию системы защиты критической инфраструктуры и регулирует импорт иностранных технологий.

Вместе с тем с точки зрения теории «сетевого общества», в котором власть конструируется путем формирования образов и фреймов, государственным акторам важно контролировать информационное пространство и контент в социальных приложениях и сервисах с целью ограничить иностранное влияние и обеспечить внутреннюю стабильность. Китай активно фильтрует поступающие потоки информации с помощью Золотого щита (*Great Firewall*) и блокирует иностранные приложения, в том числе Google, Facebook и др. (Понька, Рамич, У, 2020). Соответственно, согласно «Белой книге» по управлению Интернетом, Китай реализует

biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/ (accessed: 08.01.2021).

²⁴ U.S. Escalates Online Attacks on Russia's Power Grid // *The New York Times*. June 15, 2019. URL: <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?action=click&module=Top%20Stories&pgtype=Homepage> (accessed: 08.01.2021).

²⁵ Critical Infrastructure Sectors // *Cybersecurity and Infrastructure Security Agency*. October 21, 2020. URL: <https://www.cisa.gov/critical-infrastructure-sectors> (accessed: 08.01.2021).

²⁶ Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации. 26.07.2017. URL: <http://publication.pravo.gov.ru/Document/View/0001201707260023?index=0&rangeSize=1> (дата обращения: 08.01.2021).

²⁷ *Zhonghua renmin gongheguo wangluoanquanfa quanwen (2017 nianshishi)* // *Wu yang xian ren min zheng fu* [Закон о безопасности сети Интернет Китайской Народной Республики (вступил в силу в 2017 г.) // Народное правительство округа Мэян]. (На китайском языке). URL: <http://www.wuyang.gov.cn/fazhizaixian/falvfagui/20200419/38978.html> (дата обращения: 08.01.2021).

²⁸ *Guanjianxinxi jichusheshi anquanbaohu tiaoli // Zhonghua renmin gongheguo guowuyuanling* [Положение о защите критической информационной инфраструктуры // Постановление Госсовета Китайской Народной Республики]. 01.09.2021. URL: <https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/> (дата обращения: 08.01.2021). (На китайском языке).

²⁹ *Data Security Law of the People's Republic of China* // *The National People's Congress of the People's Republic of China*. June 10, 2021. URL: <http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml> (accessed: 08.01.2021).

³⁰ *Zhonghua renmin gongheguo geren xinxi baohufa // Quanguo renmin daibiao dahui* [Закон Китайской Народной Республики о защите личной информации // Всекитайское собрание народных представителей Китайской Народной Республики]. 20.08.2021. URL: <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml> (дата обращения: 08.01.2021). (На китайском языке).

принцип суверенитета и право на государственное управление внутренним информационным пространством³¹. Иным примером секьюритизации проблемы иностранного влияния является блокировка социальных приложений TikTok и WeChat. При президенте Д. Трампе США пытались заблокировать работу этих приложений, указывая на обработку персональных данных технологиями искусственного интеллекта, блокировку определенного контента и влияние на социальную стабильность (Williams, 2020).

В дополнение к этому следует отметить государственное управление сетью Интернет в ходе внутренних конфликтов. Государства с целью ограничить иностранное влияние, координацию протестов и распространение информации блокируют использование сети Интернет и ограничивают распространение информации. В ходе массовых протестов в 2020 г. в Беларуси правительство отключило доступ в Интернет. Также частным мобильным провайдерам было выдвинуто требование — устанавливать доступ в Интернет через Национальный центр обмена трафиком³². Это обеспечило контроль правительства Беларуси над доступом во всемирную паутину, предоставляемым частными компаниями. Таким же образом поступило правительство Республики Казахстан, ограничив доступ в Интернет на всей территории страны. Ввиду того, что протестующие использовали защищенные социальные сети, власти Казахстана отключали Интернет на время протестов с целью остановить распространение информации и координацию народных выступлений³³. Всего в 2021 г. было зафиксировано

³¹ Full Text: White Paper on the Internet in China // China Daily. June 08, 2010. URL: https://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm (accessed: 08.01.2021).

³² Белорусский «Национальный центр обмена трафиком» объяснил проблемы доступа к Интернету в стране внешней атакой // D-Russia. 12.08.2020. URL: <https://d-russia.ru/beloruskij-nacionalnyj-centr-obmena-trafikom-objasnil-problemy-dostupa-k-internetu-v-strane-vneshnej-atakoj.html> (дата обращения: 08.01.2021).

³³ Kazakhstan's Largest City Almaty, Back Online after Clashes, Blackout // Hindustan Times. January 10, 2022. URL: <https://www.hindustantimes.com/world-news/kazakhstans-largest-city-almaty-back-online-after-clashes-blackout-101641788351208.html> (accessed: 08.03.2022).

182 отключения Интернета в 34 странах, где имели место протестные движения³⁴.

Иным аспектом информационной безопасности является стабильность производственных цепочек поставок комплектующих и полупроводников. Обеспечение поставок полупроводников является ключевой задачей с точки зрения экономической и технологической безопасности. Полупроводниковый кризис, разразившийся в период пандемии COVID-19 и спровоцированный целым рядом факторов, мотивировал государства к контролю производственных цепочек и инвестированию в эту отрасль.

Китай в период обострения конкуренции с США во время президентства Д. Трампа, руководствуясь задачами национальной безопасности, начал активно работать над безопасностью в сфере полупроводников, в том числе разработками технологий и их производством. В 2020 г. Госсовет КНР предложил технологическим компаниям перенести процесс разработки (*research and development, R&D*), дизайна, производства, тестирования и упаковки полупроводников в Китай³⁵. Эта программа направлена на то, чтобы аккумулировать производство на своей территории и получить необходимые разработки в сфере полупроводников.

После прихода Д. Байдена к власти США начали активно работать над обеспечением безопасности поставок полупроводников. По распоряжению Дж. Байдена был составлен доклад, посвященный отрасли полупроводников США³⁶. Тем не менее цепочка

³⁴ Keep it On // Access now. URL: <https://www.accessnow.org/keepiton/> (accessed: 08.01.2021).

³⁵ Xinshiqi cujin jicheng dianlu chanye ruanjianchanye gaozhiliangfazhande ruogan ganzheng zhengce // Zhonghua renmin gongheguo zhongyangrenmin zhengfu [Политика Государственного совета Китая по содействию качественному развитию индустрии интегральных схем (ИС) и программного обеспечения в новую эпоху // Правительство Китайской Народной Республики]. 27.07.2020. URL: http://www.gov.cn/zhengce/content/2020-08/04/content_5532370.htm (дата обращения: 08.01.2021). (На китайском языке).

³⁶ Building Resilient Supply Chains, Revitalizing American Manufactures, and Fostering Broad-Based Growth. 100-Day Reviews under Executive Order 14017 // The White House. June 2021. URL: <https://www.whitehouse.gov/wp-content/uploads/2021/06/>

добавленной стоимости представляет собой участие ряда экономик в процессе производства. В этой связи на фоне конфронтации с Китаем США намерены вернуть на свою территорию такие производственные процессы, как сбор, упаковка и тестирование, которые ввиду меньших экономических издержек в настоящее время осуществляются в Китае. Ключевой уязвимостью здесь выступает зависимость от производственного сектора КНР и потенциальная нестабильность производственных цепочек, что может привести к нехватке полупроводников. С целью исследовать уязвимые места в этой отрасли США провели саммит с представителями частных компаний, в том числе TSMC, Samsung, Qualcomm и Apple, и предложили финансирование на создание объектов по производству чипов в США³⁷.

С появлением сети Интернет в качестве новой уязвимости стал выступать контроль над управлением корневыми серверами и фильтрация информации. Так называемые *choke points* — это критические узлы в информационном пространстве, от которых зависит функционирование информационных систем, критической инфраструктуры и обмен данными в сети Интернет³⁸. К таким критическим узлам относятся экосистемы, создаваемые технологическими корпорациями, более известными как «большая пятерка»³⁹ (Google, Amazon, Facebook, Microsoft, Apple (GAFAM)). Сервисы и приложения корпораций GAFAM используются как частными компаниями, так и государственными

учреждениями, то есть от стабильности функционирования центров обработки данных и работы служб технологической корпорации зависит безопасность объектов, на которых функционируют эти сервисы. Схожая экосистема сетевых приложений создана Китаем. В рамках такой системы платежные системы, обработка и хранение данных, распространение информации зависит от функционирования экосистем, создаваемых Alibaba, Tencent и Huawei.

Данные примеры напряженности в информационном пространстве могут стать решающим фактором для согласования норм. По аналогии с ядерной сферой, когда государства были заинтересованы в уменьшении рисков для национальной безопасности, государственные и негосударственные акторы путем конструирования кодекса поведения могут обеспечить информационную безопасность. Нарушение работы критической инфраструктуры и нестабильность цепочек поставок влечет экономические издержки для государственных акторов. Социальное и суверенное управление внутренним сегментом сети Интернет становится неотъемлемой частью национальной политики в сфере безопасности. Тем самым государственные акторы с привлечением частных сторон могут уменьшить трения в этих областях.

IV. Формирование предварительного регулирования в информационном пространстве

Конкуренция между державами определяет контроль над современными рычагами власти — глобальными правилами и институтами, стандартами и технологиями⁴⁰. Международные правила поведения в информационном пространстве также являются объектом конкуренции между державами (РФ и США) и представляют рычаг силы, который определит доминирование одного из подходов к регулированию. Как и институты, созданные после Второй мировой войны,

100-day-supply-chain-review-report.pdf (accessed: 08.01.2022).

³⁷ Readout of Biden Administration Convening to Discuss and Address Semiconductor Supply Chain // The White House. September 23, 2021. URL: <https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/23/readout-of-biden-administration-convening-to-discuss-and-address-semiconductor-supply-chain/> (accessed: 08.01.2022).

³⁸ Farrell H., Newman A. Choke Points // Harvard Business Review. January-February 2020. URL: <https://hbr.org/2020/01/choke-points> (accessed: 01.02.2022).

³⁹ Sen C. The 'Big Five' Could Destroy the Tech Ecosystem // Bloomberg. November 15, 2017. URL: <https://web.archive.org/web/20201109030953/https://www.bloomberg.com/opinion/articles/2017-11-15/the-big-five-could-destroy-the-tech-ecosystem> (accessed: 08.01.2022).

⁴⁰ Lewis J. A. Technological Competition and China // Center for Strategic and International Studies. November 30, 2018. URL: <https://www.csis.org/analysis/technological-competition-and-china> (accessed: 26.02.2022).

предрегулирование (*soft law*) информационного пространства, механизмы и институты, вырабатывающие консенсус между акторами международных отношений, становятся критическим элементом с точки зрения силы и влияния того или иного государства в международной системе.

Ведущие державы в создании предрегулирования в информационном пространстве — это США и Россия. Оба государства продвигают свои концепции международных правил поведения в информационном пространстве, что происходит в том числе в рамках ООН. Россия и США выдвинули противоположные по содержанию резолюции в рамках сессий Генеральной Ассамблеи ООН до 2021 г. (Levinson, 2021, p. 2). Со своей стороны Российская Федерация, понимая важность и значимость информационного пространства с точки зрения безопасности и экономического развития, инициировала процесс выработки и обсуждения норм поведения в рамках ООН. В 1998 г. была подготовлена первая резолюция «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» (A/RES/53/70)⁴¹. Процесс выработки предрегулирования был институционализирован в 2004 г. с созданием Группы правительственных экспертов (ГПЭ) ООН⁴². Целью ГПЭ стала выработка норм регулирования в информационном пространстве. В результате деятельности ГПЭ ООН был принят ряд докладов, однако в 2017 г. Группа не смогла прийти к консенсусу⁴³. Это стало причиной

создания нового механизма, призванного сделать процесс выработки регулирования инклюзивным: в 2018 г. Россия внесла предложение организовать новый формат определения норм и создать Рабочую группу открытого состава (РГОС)⁴⁴.

Страны «коллективного Запада» (США, Франция, Великобритания, Канада, Германия и др.) выступили против резолюции о создании РГОС. Напротив, в 2018 г. США представили собственную резолюцию по безопасности ИКТ «Поощрение ответственного поведения государств в киберпространстве» (*Advancing responsible State behaviour in cyberspace in the context of international security*), в которой был определен новый мандат действия ГПЭ ООН⁴⁵. В дополнение к этому в 2021 г. Россия и США стали главными соавторами резолюции Генеральной Ассамблеи ООН (A/RES/76/19)⁴⁶, которая признавала деятельность обоих форматов и стала свидетельством сближения позиций двух держав⁴⁷. Таким образом, ГПЭ и РГОС ООН — механизмы создания правовых режимов и продвижения концепций правового регулирования в информационном пространстве.

29.06.2017. URL: https://web.archive.org/web/20170705020039/http://www.mid.ru/ru/mezhdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/2804288 (дата обращения: 27.02.2022).

⁴⁴ «Инциденты онлайн могут привести к развязыванию полномасштабной войны офлайн» // Коммерсантъ. 06.06.2019. URL: <https://www.kommersant.ru/doc/3992579> (дата обращения: 27.02.2022).

⁴⁵ Resolution A/RES/73/266 “Advancing Responsible State Behavior in Cyberspace in the Context of International Security” // General Assembly of the United Nations. January 2, 2019. URL: https://digitallibrary.un.org/record/1658328/files/A_RES_73_266-EN.pdf (accessed: 01.02.2022).

⁴⁶ Resolution A/RES/76/19 “Developments in the Field of Information and Telecommunications in the Context of International Security, and Advancing Responsible State Behaviour in the Use of Information and Communications Technologies” // General Assembly of the United Nations. December 8, 2021. URL: <https://digitallibrary.un.org/record/3951137> (accessed: 27.02.2022).

⁴⁷ Зиновьева Е., Зинченко А. Россия и США налаживают сотрудничество в сфере информационной безопасности // Российский совет по международным делам. 09.11.2021. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/rossiya-i-ssha-nalazhivayut-sotrudnichestvo-v-sfere-informatsionnoy-bezopasnosti/> (дата обращения: 27.02.2022).

⁴¹ Resolution A/RES/53/70 “Developments in the Field of Information and Telecommunications in the Context of International Security” // General Assembly of the United Nations. January 4, 1999. URL: https://digitallibrary.un.org/record/265311/files/A_RES_53_70-EN.pdf (accessed: 01.02.2022).

⁴² Resolution A/RES/58/32 “Developments in the Field of Information and Telecommunications in the Context of International Security” // General Assembly of the United Nations. December 18, 2003. URL: <https://digitallibrary.un.org/record/507790> (accessed: 01.02.2022).

⁴³ Ответ спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских на вопрос информагентства ТАСС о состоянии международного диалога в этой сфере // Министерство иностранных дел Российской Федерации.

Россия и США в стратегиях и концепциях определяют принципы предварительного регулирования, на основе которых идет согласование норм в рамках механизмов ООН. Согласно международной стратегии для киберпространства, США выступают за принятие стандартизированных процедур надзора за кибероперациями и обеспечение доступа к сети Интернет (Davis & Lewis, 2019, p. 163). Глобальное управление киберпространством должно осуществляться с широким участием негосударственных акторов, в том числе телекоммуникационных и технологических корпораций, некоммерческих организаций и научно-технических кругов. Государства несут ответственность за защиту информационной инфраструктуры⁴⁸.

Россия и Китай продвигают право на суверенное управление информационным пространством и ограничивают доступ к компьютерной информации, находящейся на их территории. Концепция международной информационной безопасности (МИБ), подписанная государствами — членами ШОС, определяет возможность установления суверенных норм и механизмов управления своим информационным пространством и свободу в реализации своих суверенных интересов в информационной сфере (Зиновьева, 2019b). В целях защиты конституционного строя, обороны и безопасности государства могут ограничивать доступ к сети Интернет (Международная информационная безопасность: теория и практика, 2019). Ключевую роль в глобальном управлении информационным пространством играют государственные акторы, в то время как негосударственные участники выполняют консультативную роль. Важным аспектом подхода России и Китая является уважение роли всех государств в конструировании норм и правил поведения в информационном пространстве.

Исходя из вышеприведенного анализа, видно, что подходы России и США противоположны в вопросах управления Интернетом,

⁴⁸ International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World // The White House. May 2011. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed: 01.02.2022).

регулирования национального сегмента сети Интернет и его развития. Тем не менее общие интересы в сфере информационной безопасности заставляют Россию и США вести диалог по проблеме создания правового регулирования.

Таким образом, можно сделать вывод, что предрегулирование в информационном пространстве происходит через механизмы России и США, созданные в рамках ООН. Эти механизмы также выступают в качестве ключевого инструмента для продвижения своей концепции и создания правовых режимов.

V. Иерархия глобального управления в информационном пространстве

В условиях недостатка регулирования в информационном пространстве и конфликта нескольких проектов нормативно-правового регулирования этой сферы можно говорить о конкуренции за право установления норм в новом политическом пространстве.

В глобальном масштабе мощь государства традиционно оценивается по факту обладания какими-либо ресурсами, технологиями или же количественными показателями мощи (Дегтерев, 2020; Баланс сил в ключевых регионах мира..., 2021). В информационном пространстве полный комплекс таких критериев еще не был выработан. Однако основным критерием влияния, который обеспечивает лидерство в цифровом домене, является способность контролировать глобальные цепочки производства технологических продуктов, от которых зависит возможность использования и функционирования сети, проведения наступательных и оборонительных киберопераций и оказание влияния на формирование международно-правовых режимов в этой сфере.

Контроль над цепочками поставок высокотехнологичной продукции позволяет государствам влиять на доступность технологий. Так, ограничение по производству полупроводников является одним из наиболее серьезных сдерживающих факторов для Китая в технологической сфере. На данный момент передовые процессоры выпускаются несколькими компаниями: TSMC (Тайвань) — 54 % мирового рынка, Samsung (Республика

Корея) — 17 % мирового рынка, Global Foundries (США) — 7 % мирового рынка, SMIC (КНР) — 5 % мирового рынка⁴⁹. В это же время TSMC, Samsung и крупнейший производитель компьютерных чипов Intel напрямую зависят от поставок фотолитографического оборудования компании ASML (Нидерланды), которая контролирует 62 % мирового рынка и не имеет конкурентов, кроме японских компаний Canon и Nikon⁵⁰. Фактически контроль над этими компаниями играет определяющую роль в развитии глобальных технологических процессов, а наибольшее влияние на систему оказывают США, Китай, страны ЕС, Япония и Республика Корея.

Потенциалы стран в сфере кибербезопасности сложно оценить по причине защиты информации о реальных потенциалах кибервойск и проводимых кибероперациях. Однако Международный союз электросвязи (МСЭ) выпускает регулярный рейтинг кибербезопасности стран мира, согласно которому среди наиболее влиятельных акторов в информационном пространстве высоким потенциалом в сфере кибербезопасности обладают США (1-е место), Южная Корея (4-е место), Российская Федерация (5-е место), Япония (7-е место), Индия (10-е место), Турция (11-е место) и Китай (33-е место)⁵¹.

На формирование международных режимов в сфере регулирования информационного пространства на данный момент наибольшее влияние оказывают два государства — это Российская Федерация и США. Как было упомянуто ранее, эти две страны объединили вокруг себя большинство государств мира и продвигают два проекта международного

регулирования, которым на настоящий момент не было представлено весомых альтернатив.

На основе указанных критериев авторы представляют иерархию глобального управления в информационном пространстве следующим образом:

– I уровень — это полный контроль над всеми тремя сферами, который обеспечивает лидерство в глобальном управлении информационным пространством;

– II уровень — контроль над большинством сфер (двумя из трех), который позволяет оказывать наибольшее влияние на систему глобального управления информационным пространством;

– III уровень — контроль над одной из ключевых сфер, который позволяет оказывать влияние на международные отношения в информационном пространстве;

– IV уровень — опосредованный контроль, который позволяет принимать участие, но не контролировать процессы в информационном пространстве (рис. 1).

Данная модель была построена с использованием методологических наработок Т. Маурера, который предложил классификацию акторов для выявления места прокси в классификации угроз в киберпространстве (Maurer, 2018, p. 16).

На начало 2020-х гг. США остаются единственным государством, которое может одновременно контролировать глобальные цепочки производства высокотехнологичных товаров, обладают внушительным киберпотенциалом и оказывают влияние на формирование международно-правовых режимов. США стремятся сохранить свое лидерство в информационном пространстве, формируя коалицию развивающихся государств, заинтересованных в сохранении существующего миропорядка. В то же время значительное влияние на систему глобального управления оказывают Россия, Китай и страны Европейского союза, так как они обладают внушительным влиянием в информационном пространстве и формируют основные тренды. Вместе с тем важные поставщики высокотехнологичных товаров, а также страны, которые активно используют кибероперации для решения внешнеполитических задач, зачастую

⁴⁹ 2 Charts Show How Much the World Depends on Taiwan for Semiconductors // CNBC. March 15, 2021. URL: <https://www.cnbc.com/2021/03/16/2-charts-show-how-much-the-world-depends-on-taiwan-for-semiconductors.html> (accessed: 26.02.2022).

⁵⁰ How ASML Became Chipmaking's Biggest Monopoly // The Economist. February 29, 2020. URL: <https://www.economist.com/business/2020/02/29/how-asml-became-chipmakings-biggest-monopoly> (accessed: 26.02.2022).

⁵¹ Global Cybersecurity Index 2020 // International Telecommunication Union. 2020. URL: <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E/> (accessed: 26.02.2022).



Рис. 1. Иерархия системы глобального управления в информационном пространстве
 Примечание: Rule makers — акторы, оказывающие влияние на выработку международных норм, rule takers — акторы, принимающие установленные нормы и следующие им.
 Источник: составлено авторами.

выступают совместно с акторами I и II уровня, не имея возможности в одиночку воздействовать на систему глобального управления. Страны с низким уровнем технологического развития и негосударственные акторы оказывают опосредованное влияние на информационное пространство и скорее являются объектом конкуренции для более крупных акторов, а также не оказывают значительного влияния на систему глобального управления информационным пространством.

Заключение

В ходе длительного процесса эволюции угроз в информационном пространстве цифровой домен стал полноценным пространством как для межгосударственного сотрудничества, так и для конкуренции. Особая природа информационного пространства, которое одновременно находится в физической и виртуальной средах, стала причиной для изобретения принципиально новых подходов

для его регулирования и противодействия новым угрозам.

В рамках четырех этапов секьюритизации, которые были рассмотрены в статье, изменились акторы, масштаб и характер угроз, а также международно-правовые режимы в информационном пространстве. Несмотря на это, до сих пор сохраняется недостаток регулирования, который позволяет более сильным государствам оказывать большее влияние на международные процессы, формируя нормы и правила, поддерживающие их лидерство. Это порождает коренной конфликт интересов между существующим гегемоном — США и странами, которые стремятся к трансформации системы глобального управления в информационном пространстве, — РФ и КНР.

На данный момент мы можем наблюдать процесс предрегулирования в информационном пространстве, в рамках которого можно выделить несколько проектов всеобъемлющих международно-правовых режимов, которые конкурируют между собой. В то же

время страны, поддерживающие эти проекты, принимают указанные в них положения в рамках ограниченных международных форматов. В случае с США и европейскими странами — это отдельные соглашения НАТО и ЕС, а в случае с РФ и КНР — это отдельные документы в рамках ШОС и БРИКС.

Сама система глобального управления информационным пространством иерархична, и влияние на формирование новых норм и правил может оказывать ограниченный ряд государств — это США, РФ, КНР и страны ЕС. Другие участники этих процессов зача-

стую не выступают в качестве самостоятельных акторов и включены в одно из существующих объединений.

Принимая во внимание указанные факторы, можно предположить, что будет предложен альтернативный вариант государственным проектам регулирования информационного пространства — децентрализованная модель на основе блокчейн-технологий, которая позволит негосударственным акторам в большей степени влиять на систему глобального управления в информационном пространстве.

Поступила в редакцию / Received: 27.02.2022

Доработана после рецензирования / Revised: 01.04.2022

Принята к публикации / Accepted: 18.04.2022

Библиографический список

- Баланс сил в ключевых регионах мира: концептуализация и прикладной анализ* / под ред. Д. А. Дегтерева, М. А. Никулина, М. С. Рамича. Москва : РУДН, 2021.
- Данилин И. В. Америко-китайская технологическая война: риски и возможности для КНР и глобального технологического сектора // Сравнительная политика. 2020а. Т. 11, № 4. С. 160—176. <https://doi.org/10.24411/2221-3279-2020-10056>
- Данилин И. В. Концептуализация стратегии США в технологической войне против КНР: экономика, политика, технонационализм // Международная аналитика. 2020б. Т. 11, № 4. С. 21—38.
- Дегтерев Д. А. Оценка современной расстановки сил на международной арене и формирование многополярного мира. Москва : Русайнс, 2020.
- Дегтерев Д. А., Рамич М. С., Цвык А. В. США — КНР: «властный транзит» и контуры «конфликтной биполярности» // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2021. Т. 21, № 2. С. 210—231. <https://doi.org/10.22363/2313-0660-2021-21-2-210-231>
- Дегтерев Д. А., Рамич М. С., Пискунов Д. А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // Вестник международных организаций. 2021. Т. 16, № 3. С. 7—33. <https://doi.org/10.17323/1996-7845-2021-03-01>
- Зиновьева Е. С. Киберсдерживание и цифровая дилемма безопасности в американском экспертном дискурсе // Международные процессы. 2019а. Т. 17, № 3. С. 51—65. <https://doi.org/10.17994/IT.2019.17.3.58.4>
- Зиновьева Е. С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции: дис. ... д-ра полит. наук: 23.00.04. Москва : МГИМО, 2019б.
- Манойло А. В. Информационный фактор цветных революций и современных технологий демонтажа политических режимов // Вестник МГИМО-Университета. 2014. № 6 (39). С. 61—67. <https://doi.org/10.24833/2071-8160-2014-6-39-61-67>
- Международная информационная безопасность: новая геополитическая реальность* / под ред. Е. С. Зиновьевой, М. Б. Алборовоной. Москва : Аспект Пресс, 2021.
- Международная информационная безопасность: теория и практика* : в 3 т. Т. 1 / под общ. ред. А. В. Крутских. Москва : Аспект Пресс, 2019.
- Понька Т. И., Рамич М. С., У Ю. Информационная политика и информационная безопасность КНР: развитие, подходы и реализация // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2020. Т. 20, № 2. С. 382—394. <https://doi.org/10.22363/2313-0660-2020-20-2-382-394>
- Buchanan B. The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations. New York, NY : Oxford University Press, 2017.
- Buzan B. People, States, and Fear: The National Security Problem in International Relations. Brighton : Wheatsheaf Books, 1983.
- Buzan B., Hansen L. The Evolution of International Security Studies. Cambridge : Cambridge University Press, 2009.

- Buzan B., Wæver O. *Regions and Powers: The Structure of International Security*. Cambridge : Cambridge University Press, 2003. <https://doi.org/10.1017/CBO9780511491252>
- Castells M. *Communication Power*. Oxford : Oxford University Press, 2013.
- Castells M. Network Theory. A Network Theory of Power // *International Journal of Communication*. 2011. Vol. 5, no. 15. P. 773—787.
- Davis J. A., Lewis C. Beyond the United Nations Group of Governmental Experts: Norms of Responsible Nation-State Behavior in Cyberspace // *The Cyber Defense Review*. 2019. P. 161—168.
- Deibert R. J., Rohozinski R. Risking Security: Policies and Paradoxes of Cyberspace Security // *International Political Sociology*. 2010. Vol. 4, no. 1. P. 15—32. <https://doi.org/10.1111/j.1749-5687.2009.00088.x>
- Hansen L., Nissenbaum H. Digital Disaster, Cyber Security, and the Copenhagen School // *International Studies Quarterly*. 2009. Vol. 53, no. 4. P. 1155—1175. <https://doi.org/10.1111/j.1468-2478.2009.00572.x>
- Hjalmarsson O. The Securitization of Cyberspace. How the Web Was Won // *Lund University Libraries*. 2013. P. 1—28. URL: <http://lup.lub.lu.se/student-papers/record/3357990> (accessed: 26.02.2022).
- Levinson N. S. Idea Entrepreneurs: The United Nations Open-Ended Working Group & Cybersecurity // *Telecommunications Policy*. 2021. Vol. 45, no. 6. P. 1—11. <https://doi.org/10.1016/j.telpol.2021.102142>
- Maurer T. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge : Cambridge University Press, 2018. <https://doi.org/10.1017/9781316422724>
- Mueller M. L. Against Sovereignty in Cyberspace // *International Studies Review*. 2020. Vol. 22, no. 4. P. 779—801. <https://doi.org/10.1093/isr/viz044>
- Nye J. S. Deterrence and Dissuasion in Cyberspace // *International Security*. 2016. Vol. 41, no. 3. P. 44—71. https://doi.org/10.1162/ISEC_a_00266
- Nye J. S. Nuclear Lessons for Cyber Security? // *Strategic Studies Quarterly*. 2011. Vol. 5, no. 4. P. 18—38.
- Ratray G. J. *An Environmental Approach to Understanding Cyberpower* // *Cyberpower and National Security* / ed. by F. D. Kramer, S. H. Starr, L. K. Wentz. Washington, DC : National Defense University Press, Potomac Books, 2009. P. 253—274.
- Stevens T. A Cyberwar of Ideas? Deterrence and Norms in Cyberspace // *Contemporary Security Policy*. 2012. Vol. 33, no. 1. P. 148—170. <https://doi.org/10.1080/13523260.2012.659597>
- Williams R. D. Beyond Huawei and TikTok: Untangling US Concerns Over Chinese Tech Companies and Digital Security // Working Paper for the Penn Project on the Future of U.S. — *China Relations*. 2020. P. 1—44. URL: https://www.brookings.edu/wp-content/uploads/2020/10/FP_20201030_huawei_tiktok_williams.pdf (accessed: 26.02.2022).
- Xingdong F., Du L. Zhongmei keji jingzhengde weilai qushiyanjiu — quanqiu keji chuangxin qudongxiade chanye youshi zhuan yi, chongtu yuzai pingheng // *Renminluntan xueshuqianyan* [Изучение будущих тенденций китайско-американской технологической конкуренции — интенсивность, конфликт и перебалансирование, обусловленные глобальными технологическими инновациями // Народный форум Академические границы]. 2019. Vol. 4, no 24. P. 46—59. (На китайском языке). <https://doi.org/10.16619/j.cnki.rmltxsqy.2019.24.004>
- Zhao S. The US — China Rivalry in the Emerging Bipolar World: Hostility, Alignment, and Power Balance // *Journal of Contemporary China*. 2021. Vol. 31, no. 134. P. 169—185. <https://doi.org/10.1080/10670564.2021.1945733>

Сведения об авторах: *Рамич Мирзет Сафетович* — ассистент кафедры теории и истории международных отношений Российского университета дружбы народов; ORCID: 0000-0003-1479-2785; e-mail: ramich-ms@rudn.ru

Пискунов Данил Андреевич — студент кафедры теории и истории международных отношений Российского университета дружбы народов; ORCID: 0000-0002-4321-3191; e-mail: piskunov_da@mail.ru



DOI: 10.22363/2313-0660-2022-22-2-256-270

Научная статья / Research article

Большие ИИ-пространства и стратегия России в условиях санкционной войны

Р.С. Выходец  

Санкт-Петербургский государственный университет, Санкт-Петербург, Российская Федерация

 marketing812@mail.ru

Аннотация. Статья посвящена изучению роли технологического развития в области искусственного интеллекта, или ИИ, в международных политических процессах, формирования больших пространств политики в области искусственного интеллекта, а также направлений дальнейшего развития России в этой сфере. Проанализированы национальные стратегии в области ИИ, рассмотрены приоритетные для государств мира сферы и направления развития этих технологий, обеспеченность ресурсами поставленных целей, а также особенности национальной политики в области искусственного интеллекта ведущих государств мира. Сопоставляются данные об объемах финансирования разработок в области ИИ, патентной деятельности, имеющейся инфраструктуре для высокопроизводительных вычислений в странах мира, занимающих лидирующие позиции в области искусственного интеллекта. Представлен краткий обзор ключевых научно-технологических направлений, имеющих решающее значение для создания технологий ИИ следующего поколения: квантовые вычисления и нейроморфные технологии в рамках существующих крупных национальных проектов по изучению мозга. Отдельное место в работе отведено исследованию международных политических аспектов технологического развития в области искусственного интеллекта. В ракурсе воздействия политики в области ИИ на интеграционные процессы делается вывод о формировании двух пространств: первое объединяет страны Организации экономического сотрудничества и развития с безусловным лидерством США и ЕС в области научных исследований, разработок, инфраструктуры, ресурсов, международных стандартов. Второе, сдерживаемое пространство, опирается на технологическое и финансовое могущество Китая, куда начинают втягиваться страны, в том числе и Россия, для которых спектр возможностей сотрудничества с западными странами в последнее время резко сузился. Сделан вывод, что противостояние двух ИИ-пространств испытывает на себе влияние более общей тенденции декаплинга экономик США и Китая, что на глобальном уровне способствует развитию тенденций технологической изоляции. Особое внимание уделено анализу развития технологий ИИ в России — официальных документов, ведущих игроков, позиций на международном уровне. Рассматриваются возможные направления сотрудничества России с ведущими мировыми игроками, которые позволяют успешно развивать технологии ИИ и одновременно сохранять технологический суверенитет в этой сфере.

Ключевые слова: технологическое сотрудничество, искусственный интеллект, индустрия 4.0, четвертая промышленная революция, технологические пространства, декаплинг, санкционная политика

© Выходец Р.С., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

Для цитирования: *Выходец Р. С.* Большие ИИ-пространства и стратегия России в условиях санкционной войны // *Вестник Российского университета дружбы народов. Серия: Международные отношения.* 2022. Т. 22, № 2. С. 256—270. <https://doi.org/10.22363/2313-0660-2022-22-2-256-270>

Large AI Spaces and Russia's Strategy in the Context of the "Sanctions War"

Roman S. Vykhodets  

Ural Federal University, Yekaterinburg, Russian Federation

marketing812@mail.ru

Abstract. The article is devoted to the study of the role of technological development in the field of artificial intelligence (AI) in the international political processes, the formation of large policy spaces in the field of AI, as well as the development of Russia in this area. The author provides an analysis of national AI strategies, examines the priority spheres and directions of development of these technologies for different countries, the availability of resources for the goals set, and the specifics of national AI policies of the leading states. The article compares the data on the volume of funding for AI developments, patent activities, and the existing infrastructure for high-performance computing in the countries, that occupy leading positions in the field of AI. The paper provides a brief overview of the key scientific and technological areas that are crucial for the creation of next-generation AI technologies: quantum computing and neuromorphic technologies within the framework of existing major national projects on the study of the brain. The author devotes a special place to the study of international political aspects of technological development in the field of AI in the work. From the perspective of the impact of AI policy on integration processes, the conclusion is made about the formation of two spaces: the first unites the OECD countries with the unconditional leadership of the USA and the EU in the field of research, development, infrastructure, resources, and international standards. The second, restrained space, relies on the technological and financial power of China, where are starting to get involved countries, including Russia, that are facing with narrowing range of opportunities for cooperation with Western countries. The author concludes that the confrontation between the two AI spaces is influenced by a more general trend of decoupling of the economies of the USA and China, which in turn contributes to technological isolation trends at the global level. A special place in the article is devoted to the analysis of the development of AI technologies in Russia; it considers official documents, leading players, and Russia's positions at the international level. The possible directions of Russia's cooperation with the world leading players are considered, which allows to develop AI technologies and at the same time maintain technological sovereignty in this area.

Key words: technological cooperation, artificial intelligence, industry 4.0, fourth industrial revolution, technological spaces, decoupling, sanctions policy

For citation: Vykhodets, R. S. (2022). Large AI spaces and Russia's strategy in the context of the "Sanctions War". *Vestnik RUDN. International Relations*, 22(2), 256—270. <https://doi.org/10.22363/2313-0660-2022-22-2-256-270>

Введение

Одним из основных направлений развития информационных технологий на современном этапе выступают разработки в области искусственного интеллекта (ИИ) и их применение для решения все более широкого и сложного круга задач. Технологии ИИ, находясь в центре тех грандиозных социально-экономических преобразований, которые обычно связывают с четвертой промышленной революцией, в пространстве международных отношений начали приобретать ярко выраженный политический контекст. Один из

главных идеологов четвертой промышленной революции К. Шваб в своем докладе на открытии 49-го Давосского экономического форума 22 января 2019 г. подчеркнул: «Искусственный интеллект, большие данные и возможность создания технологических платформ массового использования начинают определять национальную мощь государств» (Шваб, 2019, с. 82).

Многие исследователи связывают экономический рост в XXI в. с внедрением ИИ в различные сектора промышленности. В официальных документах Европейской комиссии

подчеркивается, что ИИ в XXI в. станет основным двигателем экономического роста и повышения производительности труда, а также будет способствовать устойчивости и жизнеспособности промышленного производства¹. По прогнозам Международной корпорации данных (International Data Corporation), объем рынка ИИ-технологий к 2024 г. составит 554,3 млрд долл. США².

В этом смысле овладение технологиями ИИ, их внедрение в производство сулит государствам существенные экономические выгоды и лидирующие позиции в мировой системе разделения труда. Как указывается в итоговых материалах состоявшейся 1 декабря 2020 г. Европейской конференции по политике в области искусственного интеллекта, «эта технология важна в геополитическом отношении. Многие страны стремятся достичь глобального инновационного преимущества в области ИИ, потому что они понимают, что это фундаментальная технология, которая может повысить конкурентоспособность и помочь решить социальные проблемы»³.

Национальная политика в области ИИ

В 2017 г., когда в Канаде была принята первая в мире Национальная стратегия в области ИИ, начался процесс по официальному закреплению технологий ИИ в качестве приоритетного направления политики многих государств мира. По последним данным, уже 43 страны приняли национальные стратегии в области искусственного интеллекта и 14 — ведут работу в этом направлении (табл. 1).

Национальные стратегии различаются с точки зрения подхода, уровня детализации

предлагаемых действий и отраслевой направленности. В стратегиях применяются различные концептуальные формы: от зонтичной стратегии высокого политического уровня, охватывающей множество различных политических инициатив, до операционных стратегий с конкретными действиями и выделенным бюджетным финансированием. Существуют значительные отличия и в приоритетных направлениях государственной политики. Некоторые страны (например, Мальта и Словакия) использовали горизонтальный подход и не определили конкретных приоритетных секторов для внедрения технологий ИИ. Другие (в частности Португалия и Франция) сосредоточились на секторах экономики, которые имеют высокий потенциал роста или обеспечивают государствам конкурентные преимущества⁴.

Таблица 1

Хронология публикации национальных ИИ-стратегий в 2017—2021 гг.

Год	Государства
2017	Канада, Китай, ОАЭ, Финляндия, Япония
2018	Великобритания, Германия, Индия, Мексика, Франция, Швеция
2019	Дания, Катар, Колумбия, Литва, Люксембург, Мальта, Нидерланды, Португалия, Республика Корея, Россия, Сингапур, Словакия, США, Чехия, Эстония
2020	Болгария, Венгрия, Индонезия, Испания, Кипр, Латвия, Норвегия, Польша, Саудовская Аравия, Сербия
2021	Бразилия, Вьетнам, Ирландия, Италия, Словения, Турция, Чили
В разработке	Австралия, Австрия, Аргентина, Бельгия, Греция, Израиль, Кения, Малайзия, Новая Зеландия, Румыния, Тунис, Украина, Уругвай, Шри-Ланка

Источник: A European Approach to Artificial Intelligence // European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/strategy-artificial-intelligence> (accessed: 15.11.2021); The AI Index Report: Measuring Trends in Artificial Intelligence // Stanford University Human-Centered Artificial Intelligence. 2021. URL: <https://aiindex.stanford.edu/report/> (accessed: 16.11.2021); Government AI Readiness Index 2021 // Oxford Insights. URL: <https://www.oxfordinsights.com/government-ai-readiness-index2021> (accessed: 11.04.2022).

¹ Re-finding Industry: Defining Innovation // Publications Office of the European Union. April 24, 2018. P. 5. URL: <https://op.europa.eu/en/publication-detail/-/publication/28e1c485-476a-11e8-be1d-01aa75ed71a1> (accessed: 16.02.2022).

² IDC Forecasts Improved Growth for Global AI Market in 2021 // International Data Corporation. February 23, 2021. URL: <https://www.idc.com/getdoc.jsp?containerId=prUS47482321> (accessed: 16.02.2022).

³ Castro D. European AI Policy Conference Report — 2020 // Center for Data Innovation. April 9, 2021. URL: <https://datainnovation.org/2021/04/european-ai-policy-conference-report-2020/> (accessed: 21.12.2021).

⁴ A European Approach to Artificial Intelligence // European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/strategy-artificial-intelligence> (accessed: 15.11.2021).

Следует отметить, что лишь некоторые страны обозначили конкретные размеры финансирования принятых стратегий. Например, Китай (около 32 млрд долл. США до 2030 г.), ЕС (20 млрд евро в год, значительная часть которых приходится на Германию и Францию), США (около 30 млрд долл. США в год, из них около 24 млрд долл. США в 2020 г. пришлось на частные инвестиции), Великобритания (1,3 млрд долл. США), Индия (около 950 млн долл. США)⁵, российский федеральный проект «Искусственный интеллект» предусматривает финансирование в размере около 36,3 млрд руб. до 2024 г.⁶ В большинстве случаев данные о размерах и источниках средств на реализацию национальных стратегий в области ИИ отсутствуют, что подчеркивает декларативный характер принятых документов, которые не подразумевают фиксированной дорожной карты их реализации, а лишь иллюстрируют амбиции государства следовать в русле глобального технологического тренда.

Научно-технологическое лидерство в сфере ИИ

В настоящее время, по признанию многих специалистов, в технологической гонке за искусственным интеллектом пальму первенства удерживают ЕС, Китай и США, по одним позициям вырываясь вперед, а по каким-то аспектам догоняя друг друга. Так, например, эксперты из американского *Center for Data Innovation* в своем последнем отчете указывают, что США удерживают

лидирующие позиции в четырех из шести исследуемых ими категориях: таланты (количество высококлассных исследователей, участие в научных конференциях и др.), исследования (количество публикаций, цитирований, расходы на НИОКР и др.), разработки (количество компаний, стартапов, патентов и др.) и оборудование (производство и исследования полупроводников, производство компьютерных чипов и т. д.), а Китай является мировым лидером в таких категориях, как внедрение (число сотрудников в компаниях, связанных с ИИ) и данные (количество пользователей мобильных платежей, уровень внедрения цифровых медицинских карт, Интернет вещей и др.). При этом и Китаю, и ЕС за последнее время удалось сократить отставание от США по значительному числу параметров⁷.

Развитие ИИ-технологий тесно связано с необходимостью быстрой обработки больших массивов данных. Поэтому многие страны уделяют особое внимание созданию доступной инфраструктуры для высокопроизводительных вычислений. Например, китайский технологический гигант Tencent активно развивает платформу Angel для предприятий с потребностями в обработке больших объемов данных⁸. Для развития высокопроизводительных вычислений и разработки инновационных суперкомпьютерных технологий в 2018 г. в ЕС создано Европейское совместное предприятие по высокопроизводительным вычислениям (EuroHPC JU), объединяющее ресурсы 32 стран и частных партнеров⁹.

⁵ The AI Index Report: Measuring Trends in Artificial Intelligence // Stanford University Human-Centered Artificial Intelligence. 2021. URL: <https://aiindex.stanford.edu/report/> (accessed: 16.11.2021).

⁶ Паспорт федерального проекта Искусственный интеллект национальной программы Цифровая экономика Российской Федерации (приложение № 3 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 27.08.2020 № 17) // Судебные и нормативные акты РФ. URL: <https://sudact.ru/law/pasport-federalnogo-proekta-iskusstvennyi-intellekt-natsionalnoi-programmy/> (дата обращения: 16.11.2021).

⁷ Castro D., McLaughlin M. Who Is Winning the AI Race: China, the EU, or the United States? // Center for Data Innovation. August 19, 2019. URL: <https://datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/> (accessed: 21.12.2021).

⁸ The AI Ecosystem in China 2020 // Daxue Consulting. March, 2020. URL: <https://daxueconsulting.com/wp-content/uploads/2020/03/AI-in-China-2020-White-Paper-by-daxue-consulting-2.pdf> (accessed: 10.03.2022).

⁹ The European High Performance Computing Joint Undertaking // European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/high-performance-computing-joint-undertaking> (accessed: 21.12.2021).

По последним данным аналитиков из TOP500, мировыми лидерами по числу суперкомпьютеров и выдаваемой ими совокупной производительности являются Китай — 214 систем (42 % от общемирового количества), США — 113 систем (22,6 %), Япония — 34 системы (6,8 %). При этом по показателю совокупной производительности первое место занимают системы США — 668,7 петафлопс (27,5 % от общемирового уровня), Япония обладает наиболее производительными суперкомпьютерами в мире, выдающими в совокупности 593,7 петафлопс (24,4 %) на существенно меньшем количестве систем, чем у конкурентов, Китай занимает третье место — 566,6 петафлопс (23,3 %). Совокупные показатели стран Европейского союза — 79 систем (15,5 %) с производительностью 374,4 петафлопс (15,4 %). Россия на сегодняшний день располагает семью суперкомпьютерами, входящими в 500 наиболее производительных мировых систем, выдающими в совокупности 61,8 петафлопс (2,5 %) ¹⁰.

Качественный скачок в области высокопроизводительных вычислений многие эксперты и аналитики связывают с развитием квантовых компьютеров (Гиглави и др., 2013). В этой области пальму первенства оспаривают Китай и США. В ведущих мировых научных журналах одна за другой появляются публикации о том, что ученым из разных стран удалось добиться «квантового превосходства» на большем, чем у остальных, количестве кубитов. В 2019 г. в журнале *Nature* была опубликована статья о квантовом компьютере Sycamore компании Google, работающем на 54 кубитах (Arute et al., 2019). В конце 2020 г. появилась информация о китайском квантовом компьютере Jiuzhang на 76 кубитах, который, по мнению создателей, во много раз по своим возможностям превосходит Sycamore (Zhong et al., 2020).

Важным драйвером развития технологий ИИ выступает электронно-компонентная база. В этой сфере лидерами являются ЕС,

¹⁰ List Statistics // TOP500: The List. November, 2021. URL: <https://top500.org/statistics/list/> (accessed: 20.12.2021).

Китай и США. Так, например, среди компаний — производителей микрочипов для ИИ 14 расположены в странах ЕС, 29 — в Китае, и 62 — в США ¹¹.

Политика ведущих игроков предусматривает значительные инвестиции в собственные научные исследования и разработки. Например, Европейская комиссия на уровне ЕС запланировала на эти цели не менее 1 млрд евро в год на период до 2027 г. ¹² В США на исследования и разработки в области ИИ в 2021 г. федеральное финансирование составило 1,5 млрд долл. США ¹³.

Мировую повестку исследований и разработок в сфере ИИ определяют Китай и США, которые являются абсолютными лидерами по количеству публикаций и патентных заявок. По последним данным, в рейтинге стран по числу патентов первенство принадлежит Китаю (103,9 тыс. заявок), далее следуют США (23,5 тыс.) и Япония (12,2 тыс.). Россия находится на 15-м месте (387 заявок) ¹⁴. Если обратиться к списку 500 лучших организаций по количеству патентов в области ИИ, то Китай представлен в нем более чем 100 организациями. Для сравнения: в этот перечень входят 20 организаций из США и по 4 — из Европы и Японии. Россия в этом списке занимает седьмое место между Японией и Саудовской Аравией ¹⁵. Однако

¹¹ Castro D., McLaughlin M. Who Is Winning the AI Race: China, the EU, or the United States? // Center for Data Innovation. August 19, 2019. URL: <https://datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/> (accessed: 21.12.2021).

¹² A European Approach to Artificial Intelligence // European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/strategy-artificial-intelligence> (accessed: 15.11.2021).

¹³ The Final Report // National Security Commission on Artificial Intelligence. URL: <https://reports.nsc.gov/final-report/table-of-contents/> (accessed: 21.02.2022).

¹⁴ Развитие отдельных высокотехнологических направлений : Белая книга. Москва : НИУ «Высшая школа экономики», 2022. URL: https://www.economy.gov.ru/material/file/ba6a7585c4b23c85931aace99682ad30/belaya_kniga_2022.pdf (дата обращения: 21.02.2022).

¹⁵ WIPO Technology Trends 2019 — Artificial Intelligence. Geneva : WIPO, 2019. P. 61—63. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf (accessed: 21.02.2022).

следует отметить, что многие исследователи подчеркивают нацеленность Китая на патентную деятельность, что во многом объясняет его количественное превосходство в этой сфере. Некоторые китайские авторы указывают: «Китайские ученые опасаются, что их хорошие идеи будут восприняты западными исследователями, которые работают быстрее и обладают языковым преимуществом, чтобы быстрее описывать результаты... Мы должны научиться защищать свои собственные интересы с точки зрения прав интеллектуальной собственности, коммерциализации разработок и военных приложений» (Qiu, 2016, p. 541).

Создатели технологий ИИ с самого начала вдохновлялись фундаментальными исследованиями человеческого мозга. Один из пионеров в области ИИ Марвин Ли Мински обозначил главную цель одной из своих знаменитых работ следующим образом: «Выработать теории о том, как работает человеческий мозг, и разработать механизм, способный чувствовать и думать. Затем полученные идеи можно попытаться использовать как для изучения нас самих, так и для разработки искусственного интеллекта» (Minsky, 2006, p. 9). Сегодня в мире лишь семь стран реализуют собственные крупномасштабные проекты исследований мозга: ЕС (Human Brain Project, 2013 г.), США (BRAIN Initiative, 2013 г.), Япония (Brain/MINDS, 2013 г.), Австралия (Australian Brain Alliance, 2016 г.), Китай (China Brain Project, 2016 г.), Южная Корея (Korea Brain Initiative, 2016 г.) и Канада (Canadian Brain Research Strategy, 2017 г.) (Выходец, Рущин, 2021).

Ключевые исследовательские приоритеты национальных проектов по изучению мозга человека недвусмысленно фиксируют фундаментальные открытия нейронауки в качестве основного источника развития технологий ИИ. Например, один из руководителей China Brain Project подчеркивает, что одним из двух главных направлений проекта наряду с медициной мозга является развитие технологий ИИ (Poo et al., 2016).

Российские специалисты на протяжении многих лет подчеркивают особое значение науки о мозге для развития технологий ИИ.

Так, например, К.В. Анохин в одной из своих статей прямо указал, что создание новых систем ИИ в значительной мере обусловлено фундаментальными исследованиями в нейрофизиологии (Анохин, 2010, с. 61). Спустя 8 лет после старта первых национальных проектов по изучению мозга человека, летом 2021 г., в СМИ появились сообщения о том, что правительство РФ планирует запуск разработанной Российской академией наук программы «Мозг: здоровье, интеллект, инновации» с бюджетом 54 млрд руб. до 2029 г.¹⁶

Таким образом, сегодня определился круг стран, вышедших на мировые лидирующие позиции в области ИИ. Несмотря на то, что сегодня многие разработки с использованием ИИ получают глобальное распространение, существует непропорциональное распределение преимуществ в пользу государств, способных поддерживать весь комплекс научных и технологических инноваций в области ИИ, что укрепляет неравенство на международном уровне.

Большие ИИ-пространства

Научно-технологическое лидерство дает государству существенные преимущества в глобальной системе разделения труда и на мировой политической арене. При этом не менее существенное значение, чем занимаемая высокая ступень на технологической лестнице, в пространстве мировой политики имеет связанный с разработками в области ИИ интеграционный потенциал, который проявляется в инвестициях, образовании, транзите технологий, многосторонних инфраструктурных проектах, выработке и распространении норм, стандартов, этических принципов, подходов к обеспечению безопасности и проч. при создании и внедрении технологий ИИ.

Глобальный технологический тренд развития ИИ сегодня во многом определяет контекст двусторонних и многосторонних отношений между странами, формирует новую повестку дня в рамках интеграционных

¹⁶ Мозгоправительство // Коммерсантъ. 22.06.2021. № 105. С. 7.

проектов, а также способствует активному развитию международного сотрудничества.

На уровне международных организаций создаются экспертные группы по ИИ. Например, в феврале 2020 г. состоялось первое заседание Сети экспертов Организации экономического сотрудничества и развития (ОЭСР) по искусственному интеллекту¹⁷. В рамках Европейской комиссии создана Экспертная группа высокого уровня по искусственному интеллекту¹⁸. В ЮНЕСКО действует Специальная группа экспертов по рекомендациям по этике искусственного интеллекта¹⁹.

Активно развиваются международные площадки и крупные международные форумы. К ним относятся AI for Good Global Summit (под эгидой ООН)²⁰, AI Partnership for Defense (организаторы — Объединенный центр искусственного интеллекта и Министерство обороны США)²¹, China — ASEAN AI Summit (организаторы — Китайская Ассоциация науки и техники, Гуанси-Чжуанский автономный район)²².

В современных условиях борьба за технологическое лидерство вписывается в более широкий контекст геополитических противоречий и нередко выходит за рамки обычной

конкуренции, проявляясь в качестве одного из главных компонентов санкционной политики. Вместо всестороннего международного сотрудничества, создания открытых платформ для обмена знаниями, опытом и талантами все отчетливее проявляется тенденция к технологическому декаплингу (разделению) — концентрации технологий и технологической изоляции (Лексютина, 2020). Можно с уверенностью утверждать, что на международной арене идет процесс формирования двух больших пространств в области ИИ.

Первое пространство формируется по линии ОЭСР с безусловным лидерством США и ЕС в области научных исследований, разработок, инфраструктуры, ресурсов и международных стандартов. В мае 2019 г. странами — членами ОЭСР были приняты Принципы в отношении ИИ, разработанные на основе Рекомендаций Совета ОЭСР по искусственному интеллекту, которые закрепили стандарты национальной политики и международного сотрудничества в области развития ИИ в таких областях, как конфиденциальность, управление рисками цифровой безопасности и ответственное ведение бизнеса. Помимо членов ОЭСР к Принципам также присоединились Аргентина, Бразилия, Коста-Рика, Мальта, Перу, Румыния и Украина²³.

В июне 2020 г. создано Глобальное партнерство по искусственному интеллекту (Global Partnership on Artificial Intelligence, GPAI) — многосторонняя инициатива, разработанная в рамках G7 и на сегодняшний день объединяющая Австралию, Бельгию, Бразилию, Канаду, Чехию, Данию, Францию, Германию, Индию, Ирландию, Израиль, Италию, Японию, Мексику, Нидерланды, Новую Зеландию, Польшу, Республику Корея, Сингапур, Словению, Испанию, Швецию, Великобританию, США и ЕС. При этом Секретариат ОЭСР является постоянным наблюдателем в руководящих органах GPAI и

¹⁷ List of Participants in the OECD Expert Group on AI (AIGO) // OECD. URL: <https://oecd.ai/en/list-of-participants-oecd-expert-group-on-ai> (accessed: 03.03.2022).

¹⁸ High-level Expert Group on Artificial Intelligence // European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai> (accessed: 03.03.2022).

¹⁹ Разработка рекомендации об этических аспектах искусственного интеллекта // Организация Объединенных Наций по вопросам образования, науки и культуры. URL: <https://ru.unesco.org/artificial-intelligence/ethics> (дата обращения: 24.02.2022).

²⁰ 2020 AI for Good Global Summit to Scale AI-powered Problem Solving for Global Impact // AI for Good. URL: <https://aiforgood.itu.int/2020-ai-for-good-global-summit-to-scale-ai-powered-problem-solving-for-global-impact/> (accessed: 03.03.2022).

²¹ National Artificial Intelligence Initiative: Overseeing and Implementing the United States National AI Strategy // U.S. Government. URL: <https://www.ai.gov/> (accessed: 03.03.2022).

²² 17th China — ASEAN EXPO // ASEAN. December 1, 2020. URL: <https://asean.org/17th-china-asean-expo-china-asean-business-investment-summit-conclude/> (accessed: 03.03.2022).

²³ Recommendation of the Council on Artificial Intelligence. Legal 0449. Adopted on: 22.05.2019 // OECD Legal Instruments. URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (accessed: 28.12.2021).

направляет экспертов для участия в рабочих группах и ежегодном пленарном заседании многосторонней группы экспертов²⁴.

Эти две инициативы объединяют крупнейших мировых лидеров в области ИИ, формируя большое пространство для сотрудничества на основе общих принципов и подходов к стандартам, безопасности, ведению бизнеса и внедрению. В его рамках активно развиваются двусторонние и многосторонние форматы сотрудничества в сфере ИИ. К примеру, в июле 2018 г. Индия и ОАЭ подписали меморандум о взаимопонимании и сотрудничестве в развитии инновационных экосистем ИИ²⁵; в октябре 2019 г. Франция и Германия подписали дорожную карту для Франко-Немецкой научно-инновационной сети по ИИ²⁶; в октябре 2020 г. Индия и Япония завершили работу над соглашением, которое фокусируется на сотрудничестве в области цифровых технологий, включая 5G и ИИ²⁷; в сентябре 2020 г. США и Великобритания подписали декларацию о сотрудничестве в области ИИ²⁸.

²⁴ About GPAI // The Global Partnership on Artificial Intelligence. URL: <https://gpai.ai/about/> (accessed: 25.12.2021).

²⁵ Invest India and UAE Ministry Sign MoU for Technological Cooperation // Press Information Bureau, Government of India, Ministry of Commerce & Industry. July 27, 2018. URL: <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1540480> (accessed: 25.12.2021).

²⁶ French-German Declaration of Toulouse (16 October 2019) // Ministère de l'Europe et des Affaires étrangères. URL: <https://www.diplomatie.gouv.fr/en/country-files/germany/events/article/french-german-declaration-of-toulouse-16-oct-19> (accessed: 25.12.2021).

²⁷ India, Japan Finalise Pact for Cooperation in 5G, AI, Critical Information Infrastructure // The Economic Times. October 7, 2020. URL: <https://economictimes.indiatimes.com/news/defence/india-japan-finalise-pact-for-cooperation-in-5g-ai-critical-information-infrastructure/articleshow/78534833.cms> (accessed: 25.12.2021).

²⁸ Declaration of the United States of America and the United Kingdom of Great Britain and Northern Ireland on Cooperation in AI Research and Development // Gov.uk. September 25, 2020. URL: <https://www.gov.uk/government/publications/declaration-of-the-united-states-of-america-and-the-united-kingdom-of-great-britain-and-northern-ireland-on-cooperation-in-ai-research-and-development> (accessed: 25.12.2021).

Некоторые авторы указывают на характерную черту западного подхода к международному научно-технологическому сотрудничеству, которая заключается в появлении политически мотивированных крупномасштабных исследовательских проектов, тесно вплетенных в широкий интеграционный контекст (Ulnicane, 2020, p. 79). Например, официальные документы ЕС однозначно закрепляют приоритет сотрудничества в области ИИ с развитыми странами, занимающими сильные позиции в области НИОКР и инвестиций²⁹.

Следует подчеркнуть, что нацеленность наиболее развитых стран на первоочередное сотрудничество, прежде всего между собой, а также выдвигание собственных принципов и видение того, как должен развиваться ИИ в качестве условий сотрудничества с другими странами в этой области создает почву для выстраивания искусственных барьеров, препятствующих развитию международного сотрудничества и способствующих усилению технологической изоляции развивающихся стран. В этом аспекте некоторые исследователи указывают: «На пути поступательного развития технологий ИИ в странах Африки стоит немало препятствий. Одной из наиболее насущных задач для африканских государств является серьезная качественная модернизация системы образования с целью повышения фундаментальной цифровой грамотности» (Панцерев, 2020, с. 32).

Подобная политика во многом способствует формированию альтернативного конкурирующего пространства, в которое начинают втягиваться страны, для которых спектр возможностей для сотрудничества с коллективным Западом в последнее время резко сузился.

Второе пространство опирается на технологическое и финансовое могущество Китая. В 2015—2018 гг. в Китае на разных уровнях были приняты стратегические программы по развитию ИИ, которые обеспечили

²⁹ A European Approach to Artificial Intelligence // European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/strategy-artificial-intelligence> (accessed: 15.11.2021).

системный подход, контроль и распределение нагрузки на отрасль в целом, что в совокупности с масштабным государственным финансированием позволило Китаю занять ведущие мировые позиции в области ИИ (Решетникова, Пугачева, Лукина, 2021; Струкова, 2020).

Согласно оценкам экспертов, на глобальной арене ИИ Китай имеет преимущество в области данных и внедрения, что делает его идеальным местом для компании любой отрасли для развития новых высокотехнологичных направлений. В этом отношении вполне закономерен стремительный рост китайского рынка ИИ — более 44 % в год, в то время как общемировой показатель составляет около 26 %³⁰. Из 50 глобальных компаний ИИ с наибольшими темпами роста в мире 14 являются резидентами Китая³¹.

Цели Китая в области технологий ИИ выглядят действительно амбициозными. В табл. 2 представлены приоритетные направления Плана развития искусственного интеллекта нового поколения от 2017 г., а также плановые финансовые показатели в рамках трех контрольных дат.

Анализируя успехи Китая в области развития высоких технологий за последние 20 лет, некоторые авторы указывают, что Китай уже вышел на передовые позиции по целому ряду направлений и подготовил условия для научно-технологического «рывка» (Хейфец, 2020). Сегодня Китай достиг такого уровня технологического, финансового и компетентного могущества, что способен конвертировать свои научно-технологические достижения в международное политическое влияние.

На международном уровне сотрудничество Китая с другими странами в области ИИ зачастую включается в более широкий

контекст, связанный с высокими технологиями четвертой промышленной революции, прежде всего через инициативу «Цифровой Шелковый путь», являющуюся технологическим измерением интеграционного мегапроекта «Пояса и пути». Содержание и структура «Цифрового Шелкового пути» раскрываются в ряде стратегических документов, принятых в 2015—2019 гг.: «Сделано в Китае 2025», «Производственная супердержава», «Стратегия больших данных», «Стратегия развития облачных технологий», «Интернет плюс», «Киберсуверенитет» и др. (Лю, Авдокушин, 2019).

Таблица 2

**Плановые показатели развития ИИ в КНР
в 2020—2030 гг.**

Год	Приоритетные направления	Плановые финансовые показатели
2020	Большие данные, автономные интеллектуальные системы, роевой интеллект, гибридный расширенный интеллект, основополагающие теории ИИ	Основная отрасль ИИ — 150 млрд юаней, с учетом смежных отраслей — 1 трлн юаней
2025	Интеллектуальное производство, интеллектуальная медицина, интеллектуальный город, интеллектуальное сельское хозяйство, национальная оборона, нормативное регулирование сферы ИИ, системы оценки и контроля безопасности ИИ	Основная отрасль ИИ — 400 млрд юаней, с учетом смежных отраслей — 5 трлн юаней
2030	Социальное управление, национальная оборона, производственно-сбытовая цепочка	Основная отрасль ИИ — 1 трлн юаней, с учетом смежных отраслей — 10 трлн юаней

Источник: Hsin i tai jen kung chih neng fa chan kuei hua te t'ung chih [Уведомление Госсовета о выпуске Плана развития искусственного интеллекта нового поколения] // Правительство Китайской Народной Республики. 08.07.2017. (На китайском языке). URL: http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm (дата обращения: 10.01.2022).

По мнению некоторых авторов, «Цифровой Шелковый путь» стал одним из приоритетов Китая, направленным на снижение издержек производства, повышение глобальной конкурентоспособности китайской продукции

³⁰ The AI Ecosystem in China 2020 // Daxue Consulting. March, 2020. URL: <https://daxueconsulting.com/wp-content/uploads/2020/03/AI-in-China-2020-White-Paper-by-daxue-consulting-2.pdf> (accessed: 28.12.2021).

³¹ Global Artificial Intelligence Industry Whitepaper // Deloitte. URL: <https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/global-ai-development-white-paper.html> (accessed: 28.12.2021).

и рост торговли со странами, участвующими в инициативе (Balakin & Alikberova, 2019, p. 313). При этом при реализации «Цифрового Шелкового пути» Китай ориентируется не только на технологии следующего поколения, но также делает ставку на рынки следующего поколения. Например, более половины прироста мирового населения до 2050 г. ожидается в Африке, где Huawei построила 70 % сетей 4G. Китайский подводный кабель, соединяющий Пакистан и Джибути, станет кратчайшим интернет-соединением между Азией и Африкой — двумя регионами, где международная пропускная способность в последние годы растет наиболее быстрыми темпами. Китай даже позиционирует себя как центральное связующее звено между Нигерией и Беларусью, которые при содействии Пекина подписали контракт на предоставление услуг резервного копирования информации друг для друга (Hillman, 2021).

Такой подход самым серьезным образом усиливает международное политическое влияние Китая, поскольку позволяет претендовать на самое активное участие в установлении норм и стандартов в сфере высоких технологий и кибербезопасности. Некоторые исследователи в дискуссиях о моделях кибербезопасности уделяют особое внимание угрозам, связанным с ИИ, указывая на целый ряд таких угроз для человека и общества (Кефели, 2020, с. 47). Поэтому видение и подходы в данной сфере с опорой на финансовую и технологическую мощь позволят Китаю играть одну из ведущих ролей в определении принципов международных соглашений, например в процессе разработки общих принципов международной кибербезопасности на уровне ООН. В соответствии с ранее упомянутым «Планом развития искусственного интеллекта нового поколения» Китай активно приступает к созданию стандартов в области технологий ИИ и интеллектуальной собственности, разработке систем контроля и оценки безопасности и продвижению их в международных организациях по стандартизации, таких как ISO, Институт инженеров по электротехнике и радиоэлектронике (IEEE) и

Всемирная организация интеллектуальной собственности (WIPO)³². Именно из-за успехов Китая в сфере передовых технологий президент США Д. Трамп начал тотальную торговую и экономическую войну с Пекином, которая включает пошлины, меры экспортного контроля, репрессии против китайских ученых, а также санкции в отношении китайских высокотехнологичных компаний (Пак, 2020).

Таким образом, в настоящее время на международном уровне в области развития технологий ИИ наблюдаются процесс «замыкания» научно-технологического развития в данной сфере в рамках двух Больших технологических пространств в контексте более общей тенденции декаплинга экономик США и Китая. (Виноградов, Салицкий, Семенова, 2019). По мнению некоторых исследователей, в центре идеологии декаплинга двух крупнейших мировых экономик находятся передовые цифровые технологии (стандарт связи 5G, Интернет вещей, большие данные, искусственный интеллект и проч.), имеющие принципиальное значение для экономики будущего и — шире — для укрепления геополитического влияния Китая и США (Данилин, 2020, с. 161). Несмотря на то, что в отдельных высокотехнологичных сферах, прежде всего в производстве полупроводников и микрочипов, сохраняется зависимость от США, Китай формирует альтернативное западному пространство в сфере наиболее передовых технологий, опираясь на которое он все увереннее реализует свои геополитические амбиции.

Россия между Большими ИИ-пространствами

Формирование государственной политики в сфере ИИ началось в России в 2019 г. с принятием «Национальной стратегии разви-

³² Hsin i tai jen kung chih neng fa chan kuei hua te t'ung chih [Уведомление Госсовета о выпуске Плана развития искусственного интеллекта нового поколения] // Правительство Китайской Народной Республики. 08.07.2017. (На китайском языке). URL: http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm (дата обращения: 10.01.2022).

тия искусственного интеллекта на период до 2030 года». В развитие Стратегии в 2020 г. разработан и принят Федеральный проект «Искусственный интеллект», содержащий дорожную карту конкретных мероприятий и плановые ключевые показатели до 2024 г. Согласно документам, Россия должна занять одну из ведущих позиций в мире в этой сфере. Предполагается, что к 2024 г. Россия значительно улучшит позиции в развитии технологий ИИ, а к 2030 г. — ликвидирует отставание от развитых стран и добьется мирового лидерства в отдельных направлениях, связанных с ИИ. В Стратегии подчеркивается, что «Российская Федерация обладает существенным потенциалом для того, чтобы стать одним из международных лидеров в развитии и использовании технологий искусственного интеллекта»³³.

Основными центрами компетенций и драйверами роста технологий ИИ выступают высшие учебные заведения и крупные компании. Так, правительством РФ определены 6 исследовательских центров в сфере ИИ: Сколковский институт науки и технологий, МФТИ, Высшая школа экономики, ИТМО, Университет Иннополис, Институт системного программирования РАН. Данные организации получают 900 млн руб. бюджетного финансирования до 2024 г. для проведения НИОКР и создания прикладных решений в области ИИ. Российскими компаниями созданы отдельные продукты на основе ИИ мирового уровня — голосовой помощник Яндекса «Алиса», виртуальный ассистент Салют и решение по распознаванию речи SmartSpeech от Сбера, «Цифровая нефть» и «Когнитивный геолог» от ПАО «Газпром нефть»³⁴.

³³ Указ Президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации» № 490 от 10.10.2019 // Президент России. URL: <http://static.kremlin.ru/media/events/files/ru/AN4x6HgKWANwVtMOiPDhcbRpvd1HCCsv.pdf> (дата обращения: 10.01.2022).

³⁴ Развитие отдельных высокотехнологичных направлений : Белая книга. Москва : НИУ «Высшая школа экономики», 2022. URL: https://www.economy.gov.ru/material/file/baba7585c4b23c85931aace99682ad30/belaya_kniga_2022.pdf (дата обращения: 21.02.2022).

По данным исследования, проведенного TAdviser совместно с Ростелекомом, 85 % российских компаний уже используют ИИ-решения в бизнесе³⁵. Однако, несмотря на это, на фоне мировых лидеров позиции России в области ИИ выглядят весьма скромно. Вклад российских исследователей в общемировой объем научных публикаций по технологиям ИИ находится на уровне 1,3 %, доля патентных заявок — 0,2 %³⁶, доля России в общемировом рынке технологий ИИ составляет 0,2 %³⁷.

Вместе с тем эти невысокие показатели, равно как и достаточно амбициозные стратегические цели в области развития технологий ИИ, одинаково растворяются в ситуации неопределенности после 24 февраля 2022 г. Уже в самом начале проведения специальной военной операции Российской Федерации на территории Украины стало вполне очевидным, что ведение активных боевых действий на ограниченной территории является частью комплексного противоборства России с коллективным Западом. Россия оказалась, по сути, на передовой глобального декаплинга, который после начала боевых действий приобрел дополнительные измерения. К ранее существовавшим экономическому и технологическому измерениям добавились геоэнергетическое, валютно-финансовое, информационное и военное, и в каждом из них противоборство становится все более острым.

Спустя несколько дней после признания суверенитета Луганской (ЛНР) и Донецкой (ДНР) народных республик и начала специальной военной операции Россия стала абсолютным лидером по количеству введенных против нее санкций. Разумеется, российский

³⁵ Эффекты от внедрения решений на базе искусственного интеллекта в российских компаниях // Ростелеком, TAdviser. URL: https://www.tadviser.ru/images/8/89/ROSTELECOM_AI_0112.pdf (дата обращения: 10.01.2022).

³⁶ Там же.

³⁷ Дорожная карта развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект» // Российский фонд развития информационных технологий. URL: https://рфрит.рф/media/documents/ДК_СЦТ_ИИ.pdf (дата обращения: 10.01.2022).

высокотехнологичный сектор также оказался под ударом. Ведущие производители микропроцессоров Intel и AMD приостановили импорт в Россию своей продукции³⁸, к этим ограничениям присоединился крупнейший в мире производитель полупроводников и микросхем — тайваньская TSMC³⁹. Последний факт существенным образом обостряет имеющееся отставание России в электронно-компонентной базе. Так, будущее процессоров «Байкал» и «Эльбрус», которые должны были стать альтернативой продукции коллективного Запада, оказалось под большим вопросом в связи с решением TSMC. Подобные ограничения существуют и в отношении программного обеспечения. Кроме того, наблюдается отток высококвалифицированных IT-специалистов из России, вопрос о возвращении которых в будущем, по мнению отдельных экспертов, пока не имеет ответа⁴⁰. Существует мнение, что ситуация очень быстро изменится благодаря налаживанию логистических цепочек поставки санкционной высокотехнологической продукции через третьи страны. Однако в этом случае следует ожидать увеличения стоимости таких поставок, что может негативно отразиться на инвестиционных возможностях и конкурентоспособности российских компаний.

В условиях общемировой неопределенности, приобретающей системный характер в условиях обостряющейся санкционной политики, возможности построения долгосрочных стратегий развития, а также их теоретического осмысления достаточно ограничены. Однако следует подчеркнуть некоторые существенные моменты относительно политики России в области ИИ.

³⁸ Интегральный исход: AMD и Intel приостановили поставки своей продукции на территорию России // РБК. 27.02.2022. URL: https://www.rbc.ru/technology_and_media/27/02/2022/621a7f4f9a79473d8899b18d (дата обращения: 28.02.2022).

³⁹ Санкционный занавес: какие ограничения на импорт технологий ждут Россию // Интерфакс. 25.02.2022. URL: <https://www.interfax.ru/digital/824627> (дата обращения: 28.02.2022).

⁴⁰ Касперская: Россию покинул «табун» IT-специалистов // Газета.ru. 22.03.2022. URL: <https://www.gazeta.ru/tech/news/2022/03/22/17460589.shtm> (дата обращения: 22.03.2022).

Несмотря на имеющиеся положительные примеры сотрудничества со странами Запада в области ИИ, Россия после первых санкционных атак 2014 г. все больше тяготела к китайскому Большому ИИ-пространству. В 2022 г. данный путь представляется безальтернативным, по крайней мере в краткосрочной перспективе. При этом необходимо учитывать, что при сохранении публичного нейтралитета китайского правительства появляется все больше информации о негласном соблюдении компаниями из КНР санкционного режима в отношении России⁴¹. В случае массового подтверждения подобных фактов перед Россией встают серьезные риски оказаться в ситуации технологической автаркии с постепенно увеличивающимся разрывом в области высоких технологий.

Глобальное технологическое противостояние также играет роль центробежной силы в важнейших для России интеграционных форматах, что грозит для нее потерей в них роли лидера. Например, партнеры России по Евразийскому союзу (ЕАЭС) еще до начала острой фазы декаплинга ориентировались на китайские технологии. В частности, Huawei в мае 2018 г. опубликовала свои национальные приоритеты в области информационно-коммуникационных технологий для Республики Беларусь, включающие рекомендации по технологиям «общественной безопасности», таким как видеонаблюдение, беспилотники, системы идентификации статуса гражданина⁴².

Среди стран — участниц ЕАЭС только Россия имеет национальную Стратегию развития ИИ, включающую в качестве основных приоритетов технологическое развитие и этические аспекты применения ИИ. При этом на

⁴¹ Китайские компании тайно присоединились к санкциям Запада против России? Что известно // Telegraf.by. 10.03.2022. URL: <https://telegraf.by/ehkonomika/kitajskik-kompanii-tajno-prisoedinilis-k-sankciyam-zapada-protiv-rossii-chto-izvestno/> (дата обращения: 11.03.2022).

⁴² Cave D., Ryan F., Xu V.X. Mapping More of China's Tech Giants: AI and Surveillance // Australian Strategic Policy Institute. November 28, 2019. URL: www.aspi.org.au/report/mapping-more-chinas-tech-giants (accessed: 17.12.2021).

уровне ЕАЭС вопрос о необходимости выработки единой союзной политики в области ИИ выступает скорее предметом экспертных дискуссий и темой политических заявлений, включенных в более широкий контекст «цифровой повестки», чем сферой политического управления. Так, в феврале 2018 г. Евразийская экономическая комиссия (ЕЭК) запустила работу экспертной площадки по экономике данных и регулированию оборота данных, в качестве одного из направлений работы которой выступает разработка стратегии ЕАЭС для развития технологий ИИ⁴³. Данная ситуация создает почву для «втягивания» государств — членов ЕАЭС в орбиту политики более сильных игроков, что, в свою очередь, негативно отразится на внутреннем интеграционном потенциале. Одновременно с этим не исключен сценарий, при котором Россия из технологической метрополии в формате ЕАЭС попадет в зависимость от импорта западных и китайских технологий из стран-партнеров.

Вместе с тем некоторые эксперты указывают на зависимость многих западных стран от отдельных российских товаров, имеющих критическое значение, таких как углеводороды, зерно, удобрения, переориентация поставок которых на рынки Юго-Восточной Азии будет способствовать отказу от санкционной политики⁴⁴.

В условиях известной международной дискредитации западных валютно-финансовых инструментов повышается вероятность того, что получают дополнительный импульс развития альтернативные системы. Например, в рамках БРИКС Индия, Китай и Россия работают над системой международных платежей BRICS Pay⁴⁵, которая во многом основана на

технологиях ИИ. BRICS Pay может рассматриваться реальной альтернативой системе SWIFT не только при осуществлении покупок на территории стран-участниц, но и при торговле со странами, находящимися под западными санкциями.

Также следует указать на действия России по поддержке отрасли информационных технологий в условиях санкций. Недавно принятые политические решения предполагают бюджетные субсидии для российских компаний, работающих в IT-секторе, обнуление налога на прибыль, а также ряд мер поддержки для сотрудников таких компаний, среди которых льготная ставка по ипотеке и отсрочка от армии⁴⁶.

Помимо мобилизации внутренних ресурсов в целях прогрессивного технологического развития в области ИИ для России необходима ориентация на многостороннее сотрудничество, которое позволит развивать собственные научно-технические разработки в этой области и сохранить относительный технологический суверенитет.

Заключение

Искусственный интеллект является приоритетным направлением научно-технической политики многих государств мира. Овладение ИИ-технологиями, их внедрение в производство сулит государствам существенные экономические выгоды и лидирующие позиции в мировой системе разделения труда. Лидерами в глобальной технологической гонке за ИИ являются ЕС, Китай и США, которые обладают технологическим суверенитетом в этой области. Это подтверждается данными об объемах инвестиций, наличием собственных фундаментальных научных исследований и НИОКР, необходимой для развития ИИ-инфраструктуры и т. д.

На международной арене идет процесс формирования двух Больших пространств в

⁴³ Сборник «Цифровая повестка ЕАЭС 2016—2019—2025». Москва : Евразийская экономическая комиссия, 2019. С. 137.

⁴⁴ Глазьев С.Ю. Побеждать и строить новый мирохозяйственный уклад // Глазьев.ру. 16.04.2022. URL: <https://glazev.ru/articles/6-jekonomika/101067-pobezhdati-stroit-novuyu-mirokhozjaystvennyu-uklad> (дата обращения: 16.04.2022).

⁴⁵ BRICS Pay // Цифровой Банк БРИКС. URL: <https://digitalbankbrics.com/index.php/ru/brics-pay> (дата обращения: 11.03.2022).

⁴⁶ Указ Президента Российской Федерации от 02.03.2022 г. № 83 «О мерах по обеспечению ускоренного развития отрасли информационных технологий в Российской Федерации» // Президент России. URL: <http://kremlin.ru/acts/bank/47593> (дата обращения: 11.03.2022).

области технологий искусственного интеллекта:

— *первое* — объединяет страны ОЭСР с безусловным финансовым, технологическим и ценностно-нормативным доминированием США и ЕС;

— *второе* — пространство формируется вокруг Китая, в орбиту которого попадают страны, для которых сотрудничество с Западом осложняется вследствие широкого спектра международных противоречий; в числе таких стран находится и Россия.

Взаимодействие между двумя ИИ-пространствами следует общей тенденции декаплинга экономик США и Китая, что способствует развитию на глобальном уровне тенденций технологической изоляции и складыванию биполярной «мир-системы».

В складывающихся после 24 февраля 2022 г. условиях перед Россией встает нетривиальная задача — не остаться на обочине глобального технологического прогресса и одновременно с этим не утратить свой суверенитет в сфере высоких технологий, сохранив — пусть и в ограниченном виде — возможности многостороннего сотрудничества с ведущими игроками. Россия, находясь между двумя большими ИИ-пространствами, заинтересована в сохранении многовекторного сотрудничества в сфере ИИ и развитии собственных НИОКР в приоритетных областях, одновременно с этим предлагая партнерам уникальные разработки и возможности для кооперации в тех сферах, в которых они наиболее заинтересованы. Что касается

Китая, то в качестве такой сферы следует указать, прежде всего, проекты, связанные с геопозиционированием и управлением беспилотными аппаратами, включая военные разработки. Данное направление, очевидно, обретает синергетический эффект в совокупности с тесным сотрудничеством двух стран по построению китайской системы предупреждения о ракетном нападении (СПРН).

Ключевой возможностью для налаживания взаимодействия с ИИ-пространством Запада выступают разработки на основе искусственного интеллекта для окружающей среды. Так, в ноябре 2021 г. рабочая группа GPAI разработала стратегический документ «Изменение климата и ИИ: рекомендации для действий правительства»⁴⁷, который является новым этапом в разработке глобальной стратегии ответственного внедрения ИИ для борьбы с изменением климата и сохранения биоразнообразия в рамках Парижского соглашения.

Как представляется, наиболее важный для России аспект в развитии технологий ИИ состоит в деполитизации данной сферы или, по крайней мере, удержании ее на уровне «низкой» политики, что даст возможность поступательного развития и многостороннего сотрудничества со всеми ведущими на сегодняшний день игроками.

⁴⁷ Climate Change and AI: Recommendations for Government Action // The Global Partnership on Artificial Intelligence. November, 2021. URL: <https://gpai.ai/projects/responsible-ai/environment/climate-change-and-ai.pdf> (accessed: 10.01.2022).

Поступила в редакцию / Received: 23.08.2021
Доработана после рецензирования / Revised: 24.03.2022
Принята к публикации / Accepted: 18.04.2022

Библиографический список

- Анохин К. В. Последний великий рубеж наук о жизни // Экономические стратегии. 2010. № 11. С. 56—63.
- Виноградов А. О., Салицкий А. И., Семенова Н. К. Америко-китайская экономическая конфронтация: идеология, хронология, значение // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2019. Т. 19, № 1. С. 35—46. <https://doi.org/10.22363/2313-0660-2019-19-1-35-46>
- Выходец Р. С., Руцин Д. А. Роль Большой науки о мозге в технологическом лидерстве в области искусственного интеллекта // Общество. Среда. Развитие. 2021. № 3. С. 11—16.
- Гиглави А. В., Соколов А. В., Абдрахманова Г. И., Чулок А. А., Буров В. В. Долгосрочные тренды развития сектора информационно-коммуникационных технологий // Форсайт. 2013. Т. 7, № 3. С. 6—24. <https://doi.org/10.17323/1995-459X.2013.3.6.24>

- Данилин И. В. Американо-китайская технологическая война: риски и возможности для КНР и глобального технологического сектора // Сравнительная политика. 2020. Т. 11, № 4. С. 160—176. <https://doi.org/10.24411/2221-3279-2020-10056>
- Кефели И. Ф. Асфатроника: на пути к теории глобальной безопасности. Санкт-Петербург : ИПЦ СЗИУ РАНХиГС, 2020.
- Лексютина Я. В. Американо-китайские отношения в 2018—2019 гг.: торговая война и процесс декаплинга // Мировая экономика и международные отношения. 2020. Т. 64, № 6. С. 85—93. <https://doi.org/10.20542/0131-2227-2020-64-6-85-93>
- Лю И., Авдокушин Е. Ф. Формирование основ «цифрового шелкового пути» // Мир новой экономики. 2019. № 13. С. 62—71. <https://doi.org/10.26794/2220-6469-2019-13-4-62-71>
- Пак С. Торговая война Китая и США: что будет с китайской экономикой? // Вестник международных организаций. 2020. Т. 15, № 2. С. 213—235. <https://doi.org/10.17323/1996-7845-2020-02-10>
- Панцерев К. А. Страны Африки южнее Сахары на пути к созданию искусственного разума: миф или реальность? // Азия и Африка сегодня. 2020. № 10. С. 29—33. <https://doi.org/10.31857/S032150750011108-0>
- Решетникова М. С., Пугачева И. А., Лукина Ю. Д. Тенденции развития технологий искусственного интеллекта в КНР // Вопросы инновационной экономики. 2021. Т. 11, № 1. С. 333—350. <https://doi.org/10.18334/vines.11.1.111912>
- Струкова П. Э. Искусственный интеллект в Китае: современное состояние отрасли и тенденции развития // Вестник Санкт-Петербургского университета. Востоковедение и африканистика. 2020. Т. 12, № 4. С. 588—606. <https://doi.org/10.21638/spbu13.2020.409>
- Хейфец Б. А. Технологическое возвышение Китая: новые вызовы для России // Вопросы экономики. 2020. № 6. С. 104—120. <https://doi.org/10.32609/0042-8736-2020-6-104-120>
- Шваб К. Глобализация 4.0. Новая архитектура для четвертой промышленной революции // Евразийская интеграция: экономика, право, политика. 2019. № 1. С. 79—84.
- Arute F., Arya K., Babbush R., Bacon D., Bardin J. C. et al. Quantum Supremacy Using a Programmable Superconducting Processor // Nature. 2019. No. 574. P. 505—510. <https://doi.org/10.1038/s41586-019-1666-5>
- Balakin D. A., Alikberova A. R. Digital Silk Road in the Context of the People's Republic of China // Opción. 2019. Vol. 35, no. 22. P. 308—318.
- Hillman J. E. The Digital Silk Road: China's Quest to Wire the World and Win the Future. London : Harper Business, 2021.
- Minsky M. The Emotion Machine: Commonsense Thinking, Artificial Intelligence, and the Future of the Human Mind. New York : Simon & Schuster, 2006.
- Poo M., Du J., Ip N. Y., Xiong Z., Xu B., Tan T. China Brain Project: Basic Neuroscience, Brain Diseases, and Brain-Inspired Computing // Neuron. 2016. Vol. 92, no. 3. P. 591—596. <https://doi.org/10.1016/j.neuron.2016.10.050>
- Qiu J. Research and Development of Artificial Intelligence in China // National Science Review. 2016. Vol. 3, no. 4. P. 538—541. <https://doi.org/10.1093/nsr/nww076>
- Ulicane I. Ever-Changing Big Science and Research Infrastructures: Evolving European Union Policy // Big Science and Research Infrastructures in Europe / ed. by K. C. Cramer, O. Hallonsten. Cheltenham : Edgar Elgar, 2020. P. 76—100. <https://doi.org/10.4337/9781839100017.00010>
- Zhong H., Wang H., Deng Y., Chen M., Peng L. et al. Quantum Computational Advantage Using Photons // Science. 2020. Vol. 370, no. 6523. P. 1460—1463. <https://doi.org/10.1126/science.abe8770>

Сведения об авторе: Выходец Роман Сергеевич — кандидат философских наук, доцент кафедры теории и истории международных отношений Санкт-Петербургского государственного университета; ORCID: 0000-0002-5910-9815, e-mail: marketing812@mail.ru



DOI: 10.22363/2313-0660-2022-22-2-271-287

Research article / Научная статья

China's Digital Silk Road in the Age of the Digital Economy: Political Analysis

Guo Cheng  

People's Friendship University of Russia (RUDN University), Moscow, Russian Federation

 ivanc25@yahoo.com

Abstract. The digital economy is an increasingly important driver of the global economic growth. In recent years, regional digital cooperation has received a new tangible impetus with the launch of China's "Belt and Road" initiative (BRI). The Digital Silk Road (DSR), as the BRI's technological component, is becoming a digital bridge to promote a new type of globalization. The DSR has achieved extraordinary progress recently. It has strengthened regional cooperation in digital economy, mainly in Asia and Africa, through such channels as cross-border e-commerce and mobile financial tools, while it also reflects the global technological transformation under the Fourth Industrial Revolution in key sectors such as big data, digital currency, cloud computing and Internet of Things (IoT). Thus, the DSR provides the optimal platform for new formats and technologies, such as digital trade and digital infrastructure, which have developed rapidly in recent times. However, most countries participating in "Belt and Road" initiative are still at an early stage of digital transformation; the potential of the huge digital growth has yet to be released. Furthermore, the digital lag has become a major problem limiting economic development. This article focuses on the digital economy as a new economic model, its potential and challenges, analyzing the possible implications beyond China's DSR at both national and international levels, particularly, the role of DSR within the context of the Sino-US strategic rivalry. The methodological basis of the study covers a wide range of general scientific methods of political analysis, such as analytical, empirical, chronological, comparative, situational, narrative and descriptive. The author argues that the DSR provides a great opportunity for active multinational engagement in building a regional platform for the development of digital economy and a legal framework for digital standards and governance rules. China should focus on key sectors of the DSR, especially cross-border e-commerce, mobile financial tools, digital yuan, cloud computing and other cutting-edge components to make the DSR a more decisive initiative in global digital transformation. In promoting its own rules of digital governance, China has to be prepared to overcome difficulties and challenges that are partly the result of great power competition. The conclusion contains the results of the study and the strategic policy recommendations beyond the DSR.

Key words: digital divide, digital economy, Digital Silk Road, digital transformation, e-commerce, financial technologies, Sino-US rivalry

For citation: Cheng, Guo. (2022). China's Digital Silk Road in the age of the digital economy: Political analysis. *Vestnik RUDN. International Relations*, 22(2), 271—287. <https://doi.org/10.22363/2313-0660-2022-22-2-271-287>

Цифровой Шелковый путь Китая в эпоху цифровой экономики: политический анализ

Го Чэн  

Российский университет дружбы народов, Москва, Российская Федерация

 ivanc25@yahoo.com

Аннотация. Цифровая экономика становится все более важным фактором глобального экономического роста. Региональное сотрудничество в цифровой сфере получило ощутимый импульс в результате запуска инициативы «Пояс и путь». Цифровой Шелковый путь (ЦШП), будучи технологической частью «Пояса и

© Cheng Guo, 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

пути», выступает «цифровым мостом» в продвижении нового типа глобализации. За последние годы здесь был достигнут значительный прогресс. Благодаря ЦШП удалось укрепить региональное сотрудничество в сфере цифровой экономики, в частности в Азии и Африке, через трансграничную электронную торговлю и мобильные финансовые инструменты. ЦШП отражает глобальные технологические изменения в рамках Четвертой индустриальной революции в таких ключевых секторах, как большие данные, цифровые валюты, облачные вычисления и Интернет вещей. Как представляется, Цифровой Шелковый путь — это оптимальная платформа для новых форматов и технологий, таких как цифровая торговля и цифровая инфраструктура, которые развиваются стремительными темпами. Однако большинство стран, участвующих в инициативе «Пояс и путь», все еще находятся на начальной стадии цифровой трансформации; потенциал широкого цифрового роста в полной мере не раскрыт. Более того, отставание в сфере цифрового регулирования является основным препятствием экономического роста. Данная статья посвящена цифровой экономике как новой экономической модели, ее потенциалу и вызовам, анализу возможных последствий для китайского ЦШП на национальном и международном уровне, в том числе в контексте китайско-американского стратегического соперничества. Методологическую основу исследования составляет широкий спектр общенаучных методов политического анализа, таких как аналитический, эмпирический, хронологический, сравнительный, ситуационный, нарративный и описательный. Цифровой Шелковый путь предоставляет широкие возможности для многостороннего участия в построении региональной платформы в целях развития цифровой экономики и правовой основы для цифровых стандартов и правил управления. Китаю следует сконцентрировать свои усилия на продвижении ключевых секторов ЦШП — трансграничной электронной торговле, мобильных финансовых инструментах, цифровом юане, облачных вычислениях и других передовых компонентах. Это позволит повысить интегративную роль ЦШП в общем контексте глобальной цифровой трансформации. Продвигая собственные правила цифрового управления, Китай должен быть готов преодолевать трудности и вызовы, которые отчасти являются следствием великодержавной конкуренции. В заключении приводятся результаты исследования и рекомендации по стратегической политике.

Ключевые слова: цифровое неравенство, цифровая экономика, Цифровой Шелковый путь, цифровая трансформация, электронная торговля, финансовые технологии, американо-китайское соперничество

Для цитирования: *Cheng Guo. China's Digital Silk Road in the Age of the Digital Economy: Political Analysis // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 271—287. <https://doi.org/10.22363/2313-0660-2022-22-2-271-287>*

Introduction

The digital economy and trade have not been uniformly and clearly defined globally at the academic level, while relevant international organizations and national authorities still have disputes over the digital trade and its classification (Bukht & Heeks, 2018). At first, researchers generally believed that the digital economy was driven by the Internet (Brynjolfsson & Kahin, 2000; Lane, 1999, p. 317; Tapscott, 1996).¹ Later researchers identified three main components of the digital economy as e-business (operating process), e-business infrastructure (hardware, software, telecom, networks, etc.), and e-commerce (on-line trade).² Digitalization as a term has been

defined as the transition of businesses through the use of the digital technologies, products and services.³ Since then, the research has focused on “digitalization” and “digital transformation” to explore various cross-sectoral digitalization trends.⁴ In 2020, the OECD report offered the

Census. 2001. URL: <https://2001.isiproceedings.org/pdf/1074.PDF> (accessed: 16.04.2022).

³ Brennen S., Kreiss D. Digitalization and Digitization // Culture Digitally. September 8, 2014. URL: <http://culturedigitally.org/2014/09/digitalization-and-digitization/> (accessed: 16.04.2022).

⁴ See: Ministerial Declaration on the Digital Economy (“Cancún Declaration”) from the Meeting on the Digital Economy: Innovation, Growth and Social Prosperity // OECD. Paris: OECD Publishing, 2016. URL: <https://www.oecd.org/internet/Digital-Economy-Ministerial-Declaration-2016.pdf> (accessed: 16.04.2022); OECD Digital Economy Outlook 2017 // OECD. Paris: OECD Publishing, 2017. URL: <https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/9317011e.pdf> (accessed: 16.04.2022); Information Economy Report 2017: Digitalization, Trade and Development // UNCTAD. New York: United Nations Publications, 2017.

¹ Also see: Margherio L., Henry D., Cooke S., Montes S. The Emerging Digital Economy // U.S. Department of Commerce. 1998. URL: <https://govinfo.library.unt.edu/e-commerce/EDEREprt.pdf> (accessed: 16.02.2022).

² Mesenbourg T., Atrostic B. Measuring the US Digital Economy: Theory and Practice // U.S. Bureau of the

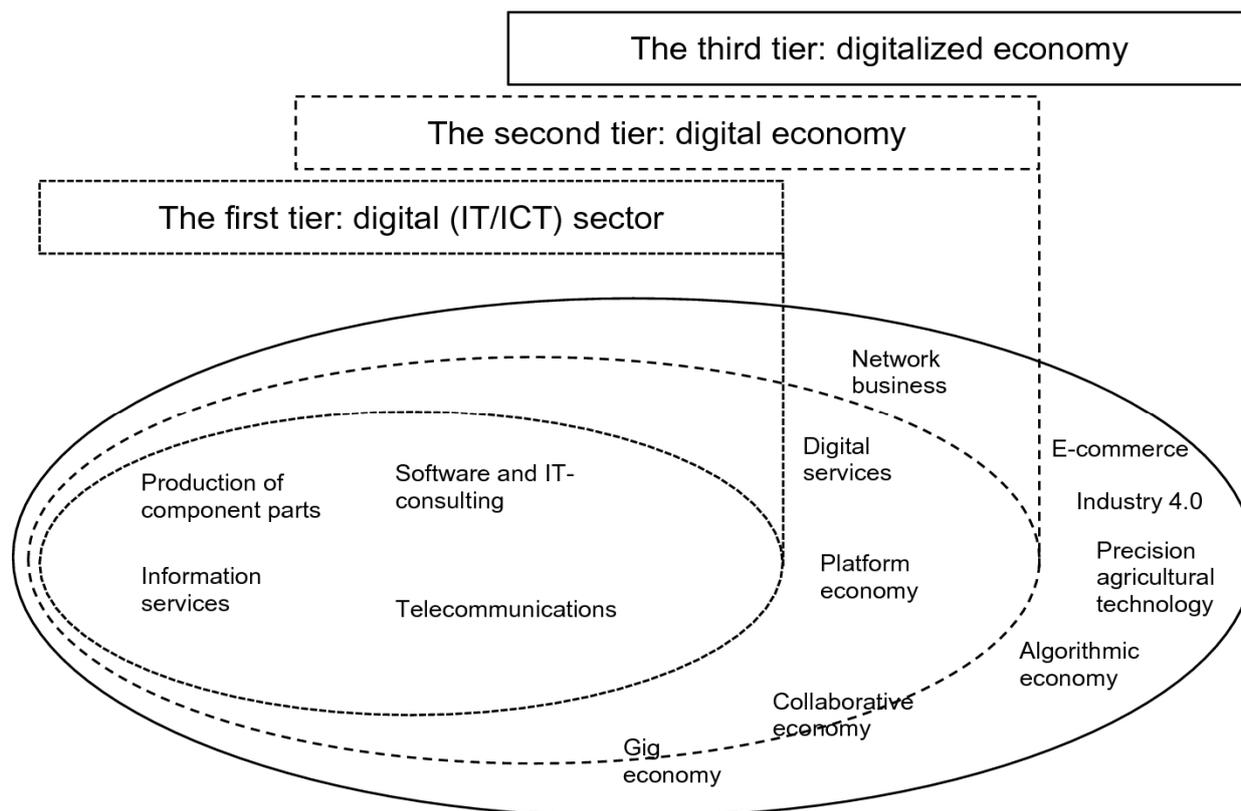


Fig. 1. The scope of the digital economy

Source: Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries // UNCTAD. New York: United Nations Publications, 2019. P. 6. URL: https://unctad.org/system/files/official-document/der2019_en.pdf (accessed: 16.04.2022).

definition from a macro perspective as bottom-up, top-down, and flexible approaches.⁵ Meanwhile, the digital trade was defined by the international organizations as “all trade that is digitally ordered and/or delivered.”⁶ The WTO report defined three components of digital trade as trade in ICT products, global e-commerce, and cross-border data transfer.⁷ The US vision of

URL: https://unctad.org/system/files/official-document/ier2017_en.pdf (accessed: 16.04.2022).

⁵ A Roadmap toward a Common Framework for Measuring the Digital Economy // OECD. 2020. URL: <https://www.oecd.org/sti/roadmap-toward-a-common-framework-for-measuring-the-digital-economy.pdf> (accessed: 16.04.2022).

⁶ Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow // UNCTAD. New York: United Nations Publications, 2021. URL: https://unctad.org/system/files/official-document/der2021_en.pdf (accessed: 16.04.2022).

⁷ World Trade Report 2018: The Future of World Trade: How Digital Technologies Are Transforming Global Commerce // World Trade Organization. 2018.

digital trade includes end-products and products and services that rely on or facilitate digital trade.⁸

The Chinese vision of digital trade refers to the trade in products, services and technologies that rely on the Internet and digital technology, use digital exchange technology as its means, and use Internet transmission as a medium for cross-border delivery tools, including digital product trade, digital service trade (Xu & Han, 2021), and digital technology trade (Ding, Liu, Zheng & Li, 2022).

In general, according to the official research, the scope of the digital economy can be interpreted as Fig. 1.

URL: https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf (accessed: 25.04.2022). See also: (Smeets, 2021).

⁸ Fefer R., Akhtar S., Sutherland M. Digital Trade and U.S. Trade Policy. Congressional Research Service // Congressional Research Service. 2021. P. 1. URL: <https://crsreports.congress.gov/product/pdf/R/R44565> (accessed: 25.04.2022).

China's Digital Silk Road: Theoretical Framework

The Digital Silk Road (DSR) is a component and a technological dimension of China's Belt and Road Initiative (BRI), a global infrastructure connectivity strategy, initiated in 2013. The DSR concept originated from the 2nd World Internet Conference in 2015, when Chairman Xi Jinping expressed China's five proposals, including speeding up the construction of global network infrastructure and promoting interconnectivity.⁹ At a sub-forum "Digital Silk Road, Cooperation and Win-win" several key issues have been discussed including launching an online platform for cultural exchanges and sharing, developing cyber economy, cyber security, and Internet governance system.¹⁰

In recent years, the DSR has gradually attracted attention of the international observers. However, there has been relatively little academic research on the issue comparing to the BRI. This reflects the general understanding among international community towards the DSR is still in formation, with few books covering the DSR as their primary topic (Hillman, 2021; Kassenova & Duprey, 2021). Based on the China's updated policy paper, some international researchers have offered their definition or understanding of the DSR goals. For example, some researchers suggested that the main components of DSR are telecommunications networks, cloud computing, e-commerce and mobile payment systems, surveillance technology, smart cities, and other high-tech areas.¹¹ Some denoted two key aspects

of the DSR as the supply of the Internet connections through submarine cables and broadband Internet and China's BeiDou satellite navigation network.¹² Although most Western researchers are skeptical about the global efforts and achievements of the DSR, questioning its security impact and implications, represented by the tech giants (such as Huawei and ZTE) activities in the relevant countries. They also believe that China's digital progress challenges Western technological leadership and accuse China of exporting its political model through technological means.¹³ There are still some researchers who believe the DSR could be beneficial to the world.¹⁴

en/tracker/networking-belt-and-road-future-digital (accessed: 13.03.2022); Assessing China's Digital Silk Road Initiative: A Transformative Approach to Technology Financing or a Danger to Freedoms? // Council on Foreign Relations. 2020. URL: <https://www.cfr.org/china-digital-silk-road/> (accessed: 16.04.2022).

¹² Linh T. Digital Trade Must be Central to Biden's 'Pivot to Asia' // The Diplomat. August 10, 2021. URL: <https://thediplomat.com/2021/08/digital-trade-must-be-central-to-bidens-pivot-to-asia/> (accessed: 16.04.2022).

¹³ See: Cheney C. China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism // Council on Foreign Relations. September 26, 2019. URL: <https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political> (accessed: 16.04.2022); Greene R., Triolo P. Will China Control the Global Internet via its Digital Silk Road? // Carnegie Endowment for International Peace. May 8, 2020. URL: <https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road> (accessed: 16.04.2022); Kurlantzick J. China's Digital Silk Road Initiative: A Boon for Developing Countries or a Danger to Freedom? // The Diplomat. December 17, 2020. URL: <https://thediplomat.com/2020/12/chinas-digital-silk-road-initiative-a-boon-for-developing-countries-or-a-danger-to-freedom/> (accessed: 16.04.2022); Wheeler A. China's Digital Silk Road (DSR): The New Frontier in the Digital Arms Race? // Silk Road Briefing. February 19, 2020. URL: <https://www.silkroadbriefing.com/news/2020/02/19/chinas-digital-silk-road-dsr-new-frontier-digital-arms-race/> (accessed: 16.04.2022); Ghiassy R., Krishnamurthy R. China's Digital Silk Road and the Global Digital Order // The Diplomat. April 13, 2021. URL: <https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/> (accessed: 16.04.2022). See also: (Tugendhat & Voo, 2021).

¹⁴ See: Agbebi M. China's Digital Silk Road and Africa's Technological Future // Council on Foreign Relations. 2022. URL: <https://www.cfr.org/sites/default>

⁹ Xi Jinping Attends Opening Ceremony of Second World Internet Conference and Delivers Keynote Speech // Embassy of the People's Republic of China in the United States of America. December 16, 2015. URL: <https://www.mfa.gov.cn/ce/ceus/eng/zgyw/t1325603.htm> (accessed: 12.03.2022).

¹⁰ Xue Lin: Hulianwang shi cishan gengjia touting [Xue Lin bates in the Field of Internet Makes Charity More Efficient and Transparent] // China Radio Network. December 17, 2015. (In Chinese). URL: http://news.cnr.cn/native/gd/20151217/t20151217_520821160.shtml (accessed: 13.03.2022).

¹¹ See: Eder T., Arcesati R., Mardell, J. Networking the "Belt and Road" — The Future is Digital // Mercator Institute for China Studies. 2019. URL: <https://mercics.org/>

The Chinese scholars believe that the DSR could play a decisive and positive role¹⁵ in a digitalized global economy (Gong & Li, 2019). Due to the large scale of the DSR, hereby the author will present the analysis only in conjunction between the DSR and the digital economy.

Research Methodology

This paper consists of a literature review supported by empirical research. The literature review is conducted to show the academic discourse on the digital economy and the DSR. The article mainly utilizes inductive and comparative methodology to articulate both the digital economy and the DSR as two related cases. The data collection focused primarily on the qualitative approach, with the data of the research containing both primary and secondary sources.

The Digital Economy in the Global Context

On a global scale, the Fourth Industrial Revolution (Industry 4.0) driven by such technologies as the Internet of Things, big data, cloud computing, information and telecommunication technologies (ICT), and artificial intelligence (AI) is having a profound impact on every corner of the socioeconomic development. The expansion of the digital economy driven by digital data and platforms (platformization) has created an immeasurable variety of new economic opportunities, leading to better of economic and social outcomes, and has become a driving force for innovation and productivity growth.¹⁶ At present, the vigorous

development of the digital economy promotes the growth of global digital trade and opens up new space for the global trade. The UN official report indicates that the scale of the digital economy accounts for about 4.5—15.5% of the global GDP.¹⁷ In the world's largest economy, the US, from 2005 to 2019, real value added of the digital economy grew at an average annual rate of 5.2% outpacing the 2.2% growth in the overall economy.¹⁸ The continuous expansion of the digital economy has pushed the world into a new digital era, and has also become the driver of a new round of globalization. Hence, the development of the digital economy has now risen to a national strategic level. It is estimated that by 2025, 24.3% of the global economy will be digital (amounting to USD 23 trillion), comparing to its share of 15.5% in 2016.¹⁹

According to the research, from 2009 to 2018, the contribution of global cross-border data flow to global economic growth was as high as 10.1%.²⁰ Cross-border data flows support almost all globalization activities, such as trade in goods and services, capital flows, and logistics. Digital trade is surpassing traditional trade and becoming a new engine of international trade and, thus, a new force of economic globalization.

In the wake of the devastating impact of the COVID-19 pandemic, the world's major economies have recognized the urgency of the digital economy and have significantly increased their investment in information technology, while strengthening the government policy support.

UNCTAD. New York : United Nations Publications, 2019. URL: https://unctad.org/system/files/official-document/der2019_en.pdf (accessed: 16.04.2022).

¹⁷ Ibid.

¹⁸ Fefer R., Akhtar S., Sutherland M. Digital Trade and U.S. Trade Policy. Congressional Research Service // Congressional Research Service. 2021. P. 1. URL: <https://crsreports.congress.gov/product/pdf/R/R44565> (accessed: 25.04.2022).

¹⁹ Digital Spillover: Measuring the True Impact of the Digital Economy // Huawei. September 5, 2017. URL: https://www.huawei.com/minisite/gci/en/digital-spillover/files/gci_digital_spillover.pdf (accessed: 16.04.2022).

²⁰ Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow // UNCTAD. New York : United Nations Publications, 2021. URL: https://unctad.org/system/files/official-document/der2021_en.pdf (accessed: 16.04.2022).

[files/pdf/Chinas%20Digital%20Silk%20Road%20and%20Africas%20Technological%20Future_FINAL.pdf](https://unctad.org/system/files/official-document/der2019_en.pdf) (accessed: 16.04.2022); Arcesati R. China's Rise in Digital Governance: Deploying Technology to Deliver Public Goods At Home and Abroad // Mercator Institute for China Studies. March 2022. URL: https://merics.org/sites/default/files/2022-03/MERICS-Primer-Digital-Governance-2021_final.pdf (accessed: 16.04.2022).

¹⁵ Hao C.J. China's Digital Silk Road: A Game Changer for Asian Economies // *The Diplomat*. April 30, 2019. URL: <https://thediplomat.com/2019/04/chinas-digital-silk-road-a-game-changer-for-asian-economies/> (accessed: 16.04.2022).

¹⁶ Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries //

For example, in February 2020, the European Commission issued its digital policy roadmap to strengthen the EU economy and improve its digital competitiveness.²¹ The digital economy is likely to start a new round of economic cycle and may become the engine of economic recovery in the post-pandemic era.

Global “Digital Divide” in the Digital Transformation Period

On the one hand, digital globalization has triggered systemic changes in the global context (Joseph, 2001, p. 335). On the other hand, digital governance rules still lag behind, with the following characteristics.

Firstly, the problem of the global “digital divide” is still prominent. For example, in least developed countries, only one in five people uses the Internet as compared to four out of five in developed countries. Furthermore, Africa and Latin America together account for less than 5% of the global colocation data centers.²² Thus, for some countries this digital gap has resulted in the “digital isolation” from the world.

Secondly, there is lack of leadership of the WTO in promoting the global digital governance rules. The world has not yet formed a unified digital governance rules framework (Aaronson & Leblond, 2018, p. 253).

Thirdly, the global digital trade rule system lacks uniformity and universal coverage. With the absence of global agreement on digital trade, the differences between the US and the EU countries on their formulation seem insurmountable. At the same time, the emerging powers, for instance, China, demand fair digital trade rules (Gao, 2021, pp. 327—331).

Fourthly, there are many barriers to digital trade rules in various countries. In order to safeguard their markets and protect their own

interests, some countries have adopted policies on digital product trade tariffs, digital product trade data flow, personal data flow policies, restrictions on FDI and export controls, etc. in the name of protecting national security (Lim, 2021, pp. 109—111).

Fifthly, lack of understanding of the legal nature of digital technologies and relevant legal regulation leads to the lack of the major legislation, regulation and supervision towards the digital trade (Sidorenko & von Arx, 2020, p. 24).

Sixth, the Sino-US strategic rivalry around digital rules and governance and technical standards has significantly intensified. Particularly, both China and the US have promoted their own cyber-sovereignty to manage information and data flows and develop intergovernmental technological ecosystems (Degterev, Ramich & Piskunov, 2021, p. 8). The US approach of a “multistakeholder, decentralized model” (Mueller, 2020) stands in sharp contrast with China’s approach of a “multilateral, centralized model” (Hong & Harwit, 2020, p. 4). Thus, the cyberspace, as the basic environment for the digital economy and digital trade, becomes the key dimension in this global digital divide.

Finally, the trend of global digital trade towards an “alliance” or “bloc” building has been further strengthened. The multilateral framework represented by the WTO has failed to produce progress on the new issues in the digital trade, which has also accelerated the trend efforts of the West to win over stakeholders to build alliances.²³

China’s Potential in the Digital Economy

In 2016, China’s digital economy amounted to 30.3% of its GDP, the added value of China’s digital economy reached USD 5.5 trillion in 2019, ranking second in the world. From 2014 to

²¹ Shaping Europe’s Digital Future // European Commission. February 19, 2020. URL: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf (accessed: 19.03.2022).

²² Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries // UNCTAD. New York : United Nations Publications, 2019. URL: https://unctad.org/system/files/official-document/der2019_en.pdf (accessed: 16.04.2022).

²³ Wu M. Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System // RTA Exchange. Geneva : ICTSD and the IDB. November, 2017. URL: <https://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final-2.pdf> (accessed: 25.04.2022).

2019, the digital economy contribution to China's GDP growth was well above 50%, and in 2019, it reached 67.7%, becoming its core driving factor.²⁴ There is a room for China's digital dividend to be transformed into the "Belt and Road" regional dividend.

The scale of China's digital economy reached USD 5.8 trillion in 2020, accounting for 38.6% of its GDP, a nominal increase of 9.7% on year-on-year basis, and an increase from 14.2% in 2005 to 38.6% in 2020. It is predicted that by 2023, 51.3% of China's GDP will be directly or indirectly related to the output of the digital economy.²⁵

The value of e-commerce transactions in China, one of the key sectors of the digital economy, has increased enormously over the past 20 years, and China has become the top global market. The market is also characterized by increasing diversity, for example, the expansion of cross-border e-commerce, the development of online-offline transactions, and the growth of e-medical services (Jiang, Zhang & Jin, 2021, pp. 141—143). In the field of cross-border e-commerce, there are many domestic market players, including e-platforms, e-payment operators, e-vendors, warehousing operators and express shippers that jointly operationalize huge numbers of online transactions and offline deliveries on a day-to-day basis (Ye, 2021, p. 154). In June 2018, China took the lead in compiling and publishing the "Framework of Standards on Cross-Border E-Commerce", which became the first guiding document for global cross-border e-commerce supervision services.²⁶

Though the COVID-19 pandemic has caused a global economic recession, China's digital technology has played an irreplaceable

²⁴ Digital Economy Development in China // The China Academy of Information and Communications Technology (CAICT). July, 2020. URL: <http://www.caict.ac.cn/english/research/whitepapers/202007/P020200728343679920779.pdf> (accessed: 25.04.2022).

²⁵ Ibid.

²⁶ Cross-Border E-Commerce: Framework of Standards // World Customs Organization. June, 2018. URL: http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/activities-and-programmes/ecommerce/wco-framework-of-standards-on-crossborder-ecommerce_en.pdf?la=en (accessed: 12.03.2022).

role not only in prevention and control of the virus, but also in the entire economic recovery process (Wang, Su, Zhang & Li, 2021). Thus, the digital economy will become the main engine of economic recovery in the post-pandemic period.

The Digital Silk Road

From China's perspective, the DSR is an important aspect of the "opening up" principle and the policy of "striving for achievement" in the new era, as well as an attempt to participate and contribute to global economic governance. The DSR strategy is also accompanied by other key initiatives such as the "Made in China 2025 (MIC 2025)", "China Standards 2035", "Internet+" and the "MCF".

At the policy level, the DSR is an organic combination of the China's determination to develop its digital economy and the BRI. It is also a natural product of promoting the "community with a shared future for mankind" in the digital age strategy. The Vision and Actions of the BRI promotion offer improved international communication, smoothing the Information Silk Road, increased information exchange and cooperation.²⁷

In 2017, at the "Belt and Road" Forum (BRF) Chairman Xi Jinping called for an innovation-driven development by strengthening cooperation in cutting-edge fields such as the digital economy, and promote big data and cloud computing, the construction of smart cities.²⁸ In September 2021, China successfully hosted the World Internet Conference BRI Internet International Cooperation Forum.²⁹

²⁷ Full Text: Vision and Actions on Jointly Building Belt and Road // Xinhua. March 28, 2015. URL: http://www.china.org.cn/china/Off_the_Wire/2015-03/28/content_35182638.htm (accessed: 14.03.2022).

²⁸ China Focus: Xi Launches Belt and Road Forum to Map Out New Global Vision // Xinhua. May 14, 2017. URL: http://www.xinhuanet.com/english/2017-05/14/c_136282137.htm (accessed: 15.03.2022).

²⁹ South — South Cooperation Event Debuts at CIFTIS-2021 International Forum on South — South Cooperation and Trade in Services Concludes Successfully // China International Center for Economic and Technical Exchanges. September 26, 2021. URL: <http://www.cicete.org.cn/article/english/NewsUpdate/202109/20210903202114.shtml> (accessed: 17.03.2022).

At the international level, the Belt and Road Digital Economy International Cooperation Initiative was launched by China in 2017 jointly with Egypt, Saudi Arabia, Serbia, Thailand, Türkiye, UAE and Laos.³⁰ To date, the memoranda of understanding (MOUs) on building the DSR have been signed between China and 22 partner countries.

One of the essential components of the DSR is the physical infrastructure such as the cross-border optical cable network. So far, progress has been witnessed in the construction of cross-border fiber optic cables carried out by China, Russia, Pakistan and other countries. Other efforts include Huawei building the “Pakistan — East Africa Cable Express (PEACE)” and China Telecom’s active involvement in the Super Transit Silk Road (STSR) internet overland cable system spanning Europe and Asia.³¹

Cross-border e-commerce can be considered one of DSR’s global benchmarks. According to official data, through the e-commerce platforms Chinese products are sold to 54 countries along the route, including such major economies as Russia, Poland, Thailand, Saudi Arabia, and Egypt.³² Cross-border e-commerce is developing rapidly internationally. Data indicate that the global cross-border e-commerce B2C market reached USD 675 billion in 2018, with an average growth rate of about 30%.³³ China and its 22 partner countries have jointly built up the

platform “DSR E-commerce”. In 2019, the total amount of China’s cross-border e-commerce trade with the participating countries increased by 87.9% year-on-year.³⁴ In 2018, China’s total retail volume of import and export commodities sold through the customs cross-border e-commerce management platform reached USD 26.6 billion, an increase of 38.3%, which most intuitively reflects the degree of internationalization of the digital economy (Liu, Osewe, Shi, Zhen & Wu, 2022).

Despite the pandemic-caused global economic recession since 2020, China has taken swift efforts in promoting its “digital diplomacy” to strengthen the global digital cooperation, boost the global digital economy development, and reinforce the implementation of the DSR in order to achieve the goal of global recovery (Table 1).

Table 1

China’s Global Efforts to promote “Digital Diplomacy”

2020	2021
September: Global Initiative on Data Security (ICT Supply Chain Security); November: China — ASEAN Digital Economy Partnership; BRICS New Industrial Revolution Partnership Innovation Base; Formulation of Smart City Guidelines	March: China — Arabian Data Security Cooperation Initiative; June: China — CELAC Cooperation Forum; July: China — ASEAN Digital Economy Development and Cooperation Forum; Guidelines on Outward Investment and Cooperation in the Digital Economy; August: China — SCO Forum on the Digital Economy; China — African Internet Development and Cooperation Forum; September: CPTPP; November: Digital Economy Partnership Agreement (DEPA)

Source: Events // The China Academy of Information and Communications Technology (CAICT). URL: <http://www.caict.ac.cn/english/events/> (accessed: 16.04.2022).

³⁰ Moody A., Yu C. Digital Silk Road Forges Strong Links // China Daily. December 5, 2017. URL: http://www.chinadaily.com.cn/business/4thwic/2017-12/05/content_35207841.htm (accessed: 19.03.2022).

³¹ Kelkar K. From Silk Threads to Fiber Optics: The Rise of China’s Digital Silk Road // Observer Research Foundation. 2018. URL: <https://www.orfonline.org/expert-speak/43102-from-silk-threads-to-fiber-optics-the-rise-of-chinas-digital-silk-road/> (accessed: 16.04.2022).

³² 2019 nian zhongguo dianzishangwu hangyefazhan xianzhuang jí shichang qianjing yanjiubaogao [Research Report on the Development and Market Prospects of China’s E-Commerce Industry in 2019] // China Business Industry Research Institute. 2019. (In Chinese). URL: <https://wk.askci.com/details/410b8e0556bd4223b5085696e00028d0/> (accessed: 19.03.2022).

³³ China — Country Commercial Guide: e-Commerce // International Trade Administration. February 3, 2021. URL: <https://www.trade.gov/country-commercial-guides/china-e-commerce> (accessed: 19.03.2022).

³⁴ Ibid.

Opportunities beyond the DSR: Implications for China

From the technological perspective, the following application scenarios have great potential in a number of practices.

Big data

For BRI countries with a well-developed big data industry, cooperation and development can be strengthened in the iterative research and development of underlying technologies (such as storage, computing and resource management) and analysis platforms (such as data collection), while the application of big data technology to marketing, risk control and network optimization could be expanded. At the same time, the cooperation will strengthen the expansion of integrated applications in vertical industries and help explore the application scenarios and business models of big data in the field of manufacturing, medical care, government affairs and public utilities.³⁵

Mobile financial functions

In terms of mobile digital infrastructure, the relevant areas along the DSR generally have complex geographical conditions, especially in many remote mountainous regions with underdeveloped regional communication facilities. Rapid development of mobile Internet has brought lower communication costs and more convenient access to the Internet for these regions, thus achieving leapfrog development. In terms of mobile finance service, digital payments through digital wallets (e-wallets) and QR codes have fundamentally shifted our lives by using personal mobile banking systems to conduct payments. The e-wallets phenomenon has driven the Chinese economy towards a “cashless” future and accelerated its digitalization process. With the help of Chinese mobile payments technology and mobile financial service model a majority of the BRI countries will have huge development

³⁵ Ma W. Could a Digital Silk Road Solve the Belt and Road’s Sustainability Problem? // World Economic Forum. September 19, 2018. URL: <https://www.weforum.org/agenda/2018/09/could-a-digital-silk-road-solve-the-belt-and-roads-sustainability-problem/> (accessed: 25.04.2022).

opportunities in financial services. In terms of mobile transportation, majority of the BRI countries have “pain points” in transportation to varying degrees. Mobile Internet and sharing economy models could quickly improve the travel experience of people in countries and regions along the route.³⁶

In particular, China is experiencing a revolution in its payment systems. Domestically, the top two Chinese mobile payment service, Alipay and WeChat pay, have seen a significant user growth in recent years (Table 2 and Fig. 2). 87% of China’s population has access to fintech apps such as WeChat Pay and Alipay, which together accounted for more than 90% of electronic payments in China as of 2021.³⁷ Globally, China aspires to lead the development of a “non-Western” payments system. Western sanction against Russia and its financial sector will further accelerate the process of internationalization of Chinese payments system.

Digital renminbi

China has been working on the digital renminbi since 2014 and is leading the way among major economies in trialing state-supported digital currency. The DSR offers great opportunities to vigorously promote the internationalization of the renminbi, especially the development of the Cross-Border Interbank Payment System (CIPS) and the digital renminbi. Particularly, China’s ban on the mining of cryptocurrencies (such as Bitcoin) in September 2021 substantiates its determination and efforts to officially launch the digital renminbi.³⁸

³⁶ Zhu V. China’s FinTech: The End of the Wild West // Institut Montaigne Policy Paper. Paris : Institut Montaigne. 2021. URL: <https://www.institutmontaigne.org/ressources/pdfs/publications/china-fintech-end-of-wild-west-note.pdf> (accessed: 25.04.2022).

³⁷ Turrin R. China’s Digital Yuan Is Not Death Knell for Alipay and WeChat Pay // South China Morning Post. February 15, 2022. URL: <https://www.scmp.com/comment/opinion/article/3166958/chinas-digital-yuan-not-death-knell-alipay-and-wechat-pay> (accessed: 24.03.2022).

³⁸ Shin F. What’s behind China’s Cryptocurrency Ban? // World Economic Forum. January 31, 2022. URL: <https://www.weforum.org/agenda/2022/01/what-s-behind-china-s-cryptocurrency-ban/> (accessed: 25.04.2022).

Table 2

Comparative Overview of Alipay and WeChat pay

Criteria	Alipay	WeChat pay
Founding company	Alibaba	Tencent
Status	Third-party mobile online payment platform	Mobile payment digital wallet
Flagship financial products	2009: Credit Card Repayment Service 2013: Yu'ebao 2017: Facial Recognition Payment Service 2019: Tourpass 2020: QR Code System containing COVID-19; Open Digital Platform	2014: Red Envelope (Hongbao) 2019: WeChat Pay HK (Transaction in Hong Kong Dollar) 2022: e-CNY available among 1 bln WeChat users
Brands	Taobao (domestic); Tmall (Tianmao) (international)	QQ; weixin
International use	Over 300 global merchants Support transactions in 18 major foreign currencies	2019: 25 countries, including Italy, Russia, South Africa, and UK
Chinese market share	2017: 54% 2020: 56% 2022: over 1 billion users	2017: 37% 2020: 39% 2022: over 1 billion users

Source: Alipay Global Merchant Portal // Alipay. URL: <https://global.alipay.com/platform/site/ihome> (accessed: 16.04.2022); Weixin zhifu menhu [WeChat Pay Portal] // WeChat Pay. (In Chinese). URL: <https://pay.weixin.qq.com/index.php/public/wechatpay> (accessed: 16.04.2022).

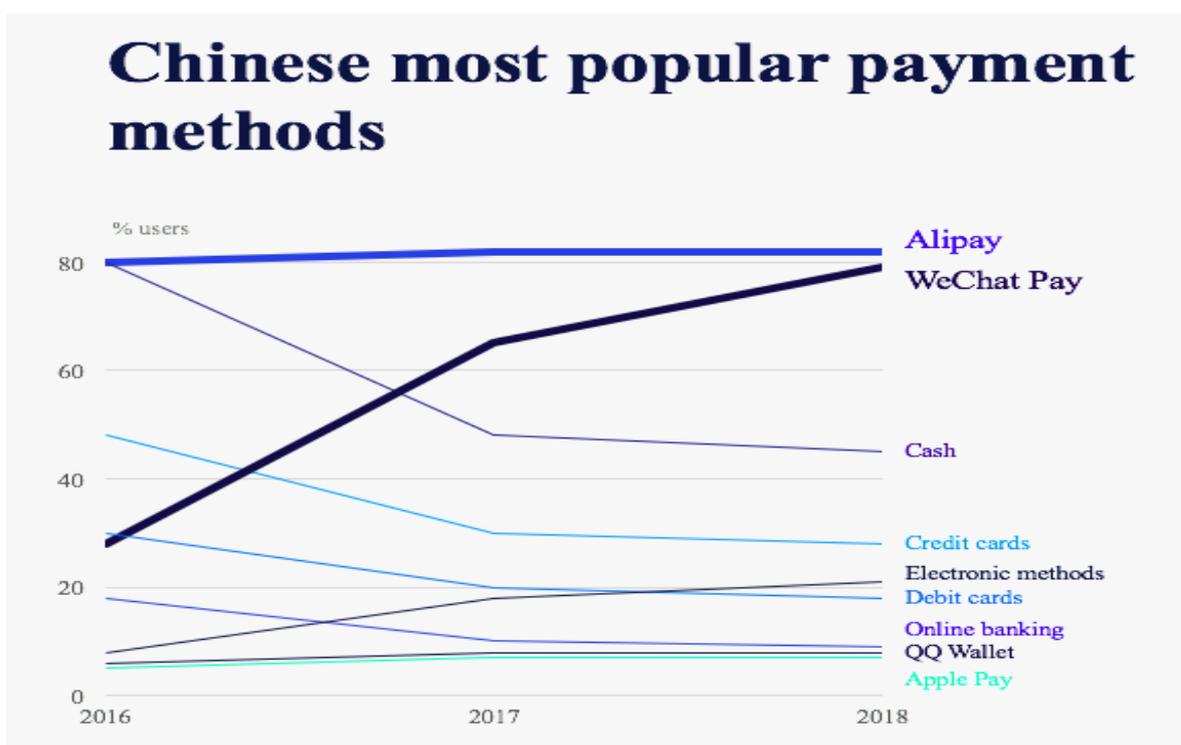


Fig. 2. Most Popular Payment Methods in China, 2016—2018

Source: Business Data Platform // Statista. URL: <https://www.statista.com/statistics/1066420/china-monthly-unique-devices-financial-apps/> (accessed: 25.03.2022).

During the pandemic, China was piloting the use of digital renminbi in its megacities (as Beijing and Shenzhen) via lotteries for domestic large-scale usage. By the end of 2021, there were 261 million users of the digital renminbi wallet who had made USD 13.8 billion worth of

transactions.³⁹ In January 2022, China launched its pilot digital renminbi through a mobile app,

³⁹ Feng C. China's Digital Currency: e-CNY Wallet Nearly Doubles User Base in Two Months to 261 Million Ahead of Winter Olympics // South China Morning Post. January 19, 2022. URL: <https://www.scmp.com/tech/tech->

e-CNY, which is available on Android and Apple application stores. Shortly after that, e-CNY was also made available for over 1 billion WeChat users ahead of the 2022 Beijing Winter Olympic Games.⁴⁰

The e-CNY clearly paves the path and guides China towards accelerating process of displacing physical cash in the long run. China's private sector could also benefit from the availability of the real time information in this digital age.

At the international level, the digitalization of the renminbi has significant potential to accelerate the use of the Chinese currency in international transactions, if the payments system outcompetes the existing infrastructure, and, finally, boosts the comprehensive internationalization of the renminbi. The BRI projects and Chinese tourists traveling around the world provide a perfect opportunity for China to promote the digital renminbi comprehensively. Furthermore, Western sanctions against Russia could offer new opportunities for the digital renminbi and its cross-border payments system.

Cloud computing technologies

With the promotion and application of cloud computing in various fields, the BRI countries have great development potential in cloud computing application fields such as industrial cloud, government cloud, and education cloud computing.

The industrial cloud computing is becoming a key element supporting the development of the manufacturing. The government affairs cloud unifies and centrally deploys the e-government affairs of various government departments and regions, which can greatly reduce IT operation and maintenance costs to build a cloud platform system for various application scenarios such as public safety management, emergency management, urban management, intelligent transportation, and social security. In addition, the developing countries under the BRI often have problems such as the scope of education popularization and the uneven quality of education. Education cloud can

break through the limitations of time and region, realizing education equity and cooperation while sharing of advantageous educational resources, and fundamentally change the way of knowledge acquisition (Lv et al., 2018).

Internet of Things (IoT)

The application and promotion of the Internet of Things (IoT) technology in the industry has further deepened the integrated application of information technology in the industrial field, providing opportunities for the DSR countries to adjust the industrial structure and promote the development of industrial integration. The increasing pressure on the environment and resources requires the DSR countries to adhere to a “green,” low-carbon, scientific and harmonious industrialization.⁴¹

Opportunities in the Application Service System

From the perspective of application services systems, first, cross-border e-commerce is the most suitable trade and business model for the DSR. In terms of the market size, cross-border e-commerce has significantly expanded recently. In addition to the traditional “Hai Tao” popular oversea markets such as the EU and Japan, and the Republic of Korea, commodities from the BRI countries have gradually become popular among the Chinese consumers in the retail sector (Liu, Osewe, Shi, Zhen & Wu, 2022).

Second, intelligent manufacturing could effectively assist the industrialization under the DSR. China and the BRI countries have similar industrial structures which could be complementary. The BRI cooperation and the “Made in China 2025” (MIC2025) initiative in the intelligent manufacturing industry has achieved good results at the practical level. There is still potential for further cooperation in high-tech products and projects such as high-speed railways.⁴²

trends/article/3163953/chinas-digital-currency-e-cny-wallet-nearly-doubles-user-base-two (accessed: 25.03.2022).

⁴⁰ Huld A. China Launches Digital Yuan App — All You Need to Know // China Briefing. April 13, 2022. URL: <https://www.china-briefing.com/news/china-launches-digital-yuan-app-what-you-need-to-know/> (accessed: 25.04.2022).

⁴¹ Ma W. Could a Digital Silk Road Solve the Belt and Road's Sustainability Problem? // World Economic Forum. September 19, 2018. URL: <https://www.weforum.org/agenda/2018/09/could-a-digital-silk-road-solve-the-belt-and-roads-sustainability-problem/> (accessed: 25.04.2022).

⁴² Ma W. Could a Digital Silk Road Solve the Belt and Road's Sustainability Problem? // World Economic Forum. September 19, 2018. URL: <https://www.weforum.org/>

Third, smart city construction is the key solution. With the information society, the population of cities has increased significantly and the scale of cities is expanding rapidly. There are no solutions to urban problems, and the effective use of modern information technology to ensure sustainable development has become urgent for the governments of all countries. Therefore, the construction of smart cities has important and far-reaching strategic significance for the DSR.⁴³

Fourth, there is a great potential for the development of telemedicine. It is the core of the “Internet + Medical Health” service and an important part of the DSR. The construction of a cross-border telemedicine service system among the BRI countries could break through the geographical restrictions, enable patients to access high-quality medical services and improve the availability of high-quality medical resources (Wang et al., 2019).

Fifth, cooperation in the field of smart education has broad prospects. Various educational resources between China and BRI countries have overcome the limitations of space and distance through network technologies radiating to a wider area and promoting more efficient utilization of educational resources. The online education has grown fast during the pandemic and demonstrated its advantages. The courses selected with no location restrictions can fully meet the needs of the citizens of the relevant countries for modern and lifelong education.⁴⁴

Challenges beyond the DSR: Implications for China

Despite the opportunities, the DSR is still in its infancy and is facing severe challenges. At the international level, centering on “digital

agenda/2018/09/could-a-digital-silk-road-solve-the-belt-and-roads-sustainability-problem/ (accessed: 25.04.2022).

⁴³ Siacor J. Smart Technology to Make China’s Belt and Road Initiative Sustainable // OpenGov. March 30, 2022. URL: <https://opengovasia.com/smart-technology-to-make-chinas-belt-and-road-green-initiative-sustainable/> (accessed: 25.04.2022).

⁴⁴ Zhou T. From “Hardware” to “Human-ware” // China Daily. March 8, 2022. URL: <https://www.chinadaily.com.cn/a/202203/08/WS62269f94a310cdd39bc8b0b9.html> (accessed: 25.04.2022).

sovereignty” and related geopolitical and economic interests, such challenges to the DSR have become increasingly prominent.

The Sino-US strategic rivalry has dramatically transformed the bilateral relations and become a megatrend of the contemporary international relations. The technological dimension of this rivalry, concerning technological dominance in the digital age, runs deeper and outlasts any putative resolution of the Sino-US trade war (Degterev, Ramich & Tsvyk, 2021, pp. 221—223). The DSR has become a new frontier in this technological competition. Various definitions as “techno-nationalism” and “techno-globalization” profoundly reflect that the “technopolitical spheres of influence” caused by digitalization are no longer purely territorial, but still allow geopolitical power to be projected and international dependencies to be cemented (Luo, 2022, pp. 4—6).

The Trump administration undertook comprehensive decoupling efforts by launching the “techonomic war” to counter China. Furthermore, it defined China’s technological rise as the national security threat. Its main efforts evidently reflect its intention to force China to abandon its “Made in China 2025” policy and compete with the DSR. Meanwhile, the Trump administration listed the cutting-edge technologies as quantum science, AI, and 5G communications as top national R&D priorities. Overall, the Trump administration focused more on countering China’s high-tech manufacturing sector rather than specifically countering the DSR (Table 3, 4).

As shown in Table 3, the Trump administration has sought to intensify regulatory efforts to block China’s access to advanced US technology by reforming the Committee on Foreign Investment in the United States (CFIUS) review mechanism, modernizing the foreign investment review process and export control system. Particularly, the Entity List blacklists the top Chinese high-tech suppliers. Thus, Huawei is the global leading producer in multiple sectors as ICT, IoT, cloud computing, and artificial intelligence (AI). Hikvision and Dahua Technology are the top global suppliers of the video surveillance technologies. SenseTime Group is the world’s most funded AI startup and

Table 3

The Trump Administration Major China-related Legislation and Chinese Companies Targeted, 2017—2021

Measures	2017	2018	2019	2020	2021
Export control		Export Control Reform Act		Export Controls on Artificial Intelligence (AI) Software	
Investment restriction	CFIUS blocked the Ant Financial (Alibaba) purchase MoneyGram bid	Foreign Investment Risk Review Modernization Act		Executive Order (EO) 13959 (31 Chinese companies, including China Telecom Corp Ltd; China Mobile Ltd; Hikvision)	
Export administration regulations entity list			May: HUAWEI, ZTE June: Sugon; the Wuxi Jiangnan Institute of Computing Technology; Higon; Chengdu Haiguang Integrated Circuit; Chengdu Haiguang Microelectronics Technology; October: Dahua Technology; HikVision, SenseTime Group; Megvii	SMIC	Total 420 Chinese companies and subsidiaries by the end of term
Information and communications technology	EO 13794 (Establishment of US technology Council)		EO 13873 (Huawei, ZTE)	EO 13913 (Huawei, ZTE)	
Applications and software bans (including mobile payment apps)				EO 13942 (TikTok) EO 13943 (WeChat)	EO 13971 (WeChat Pay; Alipay; QQ Wallet)
Delisting from stock exchanges				Holding Foreign Companies Accountable Act (Alibaba, JD.Com, Pinduoduo, PetroChina, Netease)	

Source: The US — China Trade War: A Timeline // China Briefing. April 25, 2020. URL: <https://www.china-briefing.com/news/the-us-china-trade-war-a-timeline/> (accessed: 16.04.2022).

is renowned for powerful facial recognition systems. SMIC is the global top semiconductor supplier and chip maker. Besides the ban on these Chinese hardware companies, the Trump administration also focused on countering China's rising fintech through banning Chinese software companies, the key reason of its ban on WeChat and Alibaba is their payments system. Facebook⁴⁵ and other US tech giants supported limiting the use of the WeChat and TikTok electronic payments

⁴⁵ On March 21, 2022, the Tverskoy District Court of Moscow satisfied the claim of the Prosecutor General's Office of the Russian Federation and recognized the activities of the social networks Instagram and Facebook, owned by Meta, as extremist, banning their work in Russia. — *Editor's note*.

systems. President Trump also focused on the digital renminbi challenge to the US banking system calling for the digitalization of the US dollar to compete with China (see Table 4).

If President Trump's techonomic war with China marked a starting point of the Sino-US high-tech competition, President Biden's goal is to win this competition by various means. During the campaign, Biden advocated much increasing investments in the technological sphere and improving digital access. Since taking office, President Biden has initiated a fundamental tactical change in continuing this techonomic war by prioritizing countering China's BRI and DSR specifically and strengthening the US digital economy capacity (Table 5).

Table 4

The Trump Administration Domestic Legislation on High-Tech and Digital Trade Agreements

Measures	2018	2019	2020
Domestic	National Quantum Initiative Act: Quantum Computing	EO 13859; American AI Initiative: American Leadership in Artificial Intelligence; American Broadband Initiative (ABI): Deployment of Broadband Internet across Rural America	Secure 5G and Beyond Act: U.S. Leadership in 5G Technology
International	Infrastructure Transaction and Assistance Network (ITAN); Digital Connectivity and Cybersecurity Partnership (DCCP); Asia EDGE;	Blue Dot Network (BDN); U.S. — Japan Digital Trade Agreement	Clean Network Initiative

Source: Presidential Actions // The Trump White House Archives. URL: <https://trumpwhitehouse.archives.gov/presidential-actions/> (accessed: 16.04.2022).

Table 5

The Biden Administration’s Main Domestic High-Tech Legislation and Global Initiatives

Actions	2021	2022
Domestic	S.1169: Strategic Competition Act of 2021 (First ever Official Act calling for the Great Power Competition, particularly countering China’s BRI); S.1260: US Innovation and Competition Act of 2021 (Maintaining the US Technological Supremacy and Countering China’s Rising Tech Power); EO 14005; EO 14017 (Supply Chain); EO 14007 (High-Tech); EO 14028 (Cybersecurity); EO 14029 (Technical Amendment); EO 14032 (Security of Chinese Companies Investment); EO 14034 (Big Data); EO 14036 (US Economy Competition)	EO 14067 (Digital Assets, particularly Digital USD)
International	Build Back Better World (B3W)	

Source: Presidential Actions // The White House. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/> (accessed: 16.04.2022).

Domestically, the Biden administration enacted investments in the US digital potential, which demonstrates that the digital trade and transformation form a crucial part of the Biden administration’s economic policy. The Build Back Better World (B3W) plan promised infrastructural investments of USD 2 trillion over eight years, with USD 100 million per year directed towards broadband infrastructure. The COVID-19 pandemic laid bare the digital divide between the Americans, particularly in rural communities. These investments plan to provide affordable digital access to the 30% of Americans.⁴⁶ Particularly, President Biden initiated real actions to strengthen the US digital economy through his executive order on big data

⁴⁶ He W. Rivalry Must Not Dominate B3W // China Daily. November 30, 2021. URL: <http://global.chinadaily.com.cn/a/202111/30/WS61a56012a310cdd39bc783ba.html> (accessed: 25.04.2022).

and other digital assets including a U.S. Central Bank Digital Currency.⁴⁷

Internationally, in June 2021, the US-led G7 finally announced the global infrastructure alternative, the B3W Partnership, which is considered by the majority of analysts as the first ever US-led global initiative to counter China’s BRI.⁴⁸ The B3W proposal echoes the DSR in aiming to increase global digital connectivity. It is Biden’s greatest move to mobilize the private-sector capital of the US and its allies in digital technology, ideology (democratic values), and

⁴⁷ Avery D. Biden’s ‘Digital Dollar’: Could This Be the US’ Answer to Bitcoin? // CNET. April 5, 2022. URL: <https://www.cnet.com/personal-finance/crypto/biden-digital-dollar-governments-answer-to-bitcoin/> (accessed: 25.04.2022).

⁴⁸ Johnson K. Belt and Road Meets Build Back Better // Foreign Policy. October 4, 2021. URL: <https://foreignpolicy.com/2021/10/04/belt-and-road-initiative-bri-build-back-better-us-china-competition-west/> (accessed: 16.04.2022).

standards. The Biden administration has considered a regional digital economy initiative, particularly for the Indo-Pacific.⁴⁹ In general, the Biden administration has undertaken swift effort through its international network to strengthen the blockade of China's digital technology and counterbalance China in terms of technical standards and international rules.

As the pessimistic expectations of global economic growth have intensified, the global industrial and supply chain system is facing the risk of rupture far beyond that experienced due to the Sino-US trade war since 2018. The US has pursued the pushback policy against China, and the decoupling is rampant. The US has also mobilized its allies to repeatedly suppress China's high-tech sectors while damaging the global trade system. The COVID-19 lockdown and restrictive measures have seriously affected the cross-border flow of people, goods and investments, further inhibited the vitality and impetus of economic growth. In addition, increased uncertainty in the global political and economic expectations would exacerbate differences and conflicts between the governments.

The DSR still lacks relevant digital governance rules and frameworks. At present, the global digital governance rules are still in its infancy. The US and the EU have their own rules and different interests and have not yet formed a unified and widely recognized multilateral system. Multilateral frameworks such as the WTO have failed to achieve substantial progress in increasing cross-border data flow, privacy protection, and digital service market access. In addition, China's digital economy rules focus on the facilitation of global logistics, cross-border payments and other services, and cross-border trade in goods, however the legal system for digital intellectual property protection is not yet perfect, and the shortcomings of digital governance rules may bring greater challenges to the DSR (Luo, 2022).

China's digital governance rule system is still imperfect. The basic system related to the

development of the digital trade is not yet perfect, and government efforts to spearhead negotiations and discourse are insufficient. Currently, China has signed 19 FTAs with 26 countries and regions, but only 7 FTAs concluded after 2015 include e-commerce chapters with limited scope, and another 8 include e-commerce chapters (Eckhardt & Wang, 2021). These e-commerce chapters cover traditional e-commerce issues such as digital product treatment and digital facilitation, but do not cover such issues as cross-border data flow, personal privacy protection, source code, intellectual property rights, and digital service market access. There is a lack of the systematic design of digital trade rules and negotiation strategies and also a large gap between the main positions and high-standard rules, which results in a relatively weak position in the negotiation game of multilateral and bilateral digital trade rules (Liu, Osewe, Shi, Zhen & Wu, 2022).

Conclusion

This paper provides a comprehensive analysis of China's DSR in the digital economy. In particular, this paper discusses the DSR's achievements, opportunities and challenges ahead. There are also several policy recommendations for building an even better DSR in the long run.

Firstly, China needs to promote the interconnection through the digital infrastructure of the DSR and accelerate the integration of rules and standards, actively share experience in digital infrastructure and bridge the digital infrastructure gap under the DSR. China needs to utilize its advantages in 5G, R&D and AI technology application to guide and support Chinese companies to participate more in the digital infrastructure construction. The scope of cooperation in the Internet of Things, intelligent interconnection, 5G and other fields should be expanded. Furthermore, China needs to accelerate an in-depth integration of traditional infrastructure such as subways, ports, and railways in BRI countries, with the new-generation information technologies such as the Internet, big data, and cloud computing and actively promote smart cities at the global level.

Secondly, China needs to take the opportunity of multilateral and bilateral

⁴⁹ Halpert M. Sources: Digital Trade Deal under 'Serious' Interagency Consideration // Inside Trade. November 2, 2021. URL: <https://insidetradetrade.com/daily-news/sources-digital-trade-deal-under-%E2%80%98serious%E2%80%99-interagency-consideration> (accessed: 25.03.2022).

platforms to build and share the framework of digital governance rules under the DSR. Digital governance is a new field of global governance, and the DSR should be used to jointly formulate a coordinated digital trade development mechanism and global digital governance rules from the perspective of exploring digital governance experience and coordinating interests, while promoting multilateral consultations in order to accelerate the pace of negotiations on issues related to high-standard digital trade rules. This may gradually narrow the scope of what is acceptable and what is not in the digital trade regulation.

Thirdly, China needs to focus more on exploring the cross-border e-commerce rules and standards. The BRI countries have obvious differences in import and export tariffs, logistics and transportation, package release, intellectual property protection, and credit reporting systems. Speeding up the establishment of unified rules is a top priority for all parties. It is urgent that China further expand the Electronic World Trade Platform (eWTP) and form a widely applicable eWTP standardization rule system. Particularly, China needs to focus on selecting qualified

eWTP overseas markets, such as Malaysia, Rwanda, Ethiopia, and Belgium etc., to establish important digital trade platforms and hubs there (Johnston, 2021).

Fourthly, China needs to take the promotion of the DSR digital governance rules as an opportunity to speed up the improvement of basic domestic institutional arrangements by formulating and improving the basic digital trade rules, accelerating digital trade-related legislation, and gradually forming a rules-based supervision system. In addition, it is necessary to establish and improve the data market and reduce institutional obstacles by improving the cross-border data flow system, promoting the two-way flow of data, and effectively safeguarding the national digital sovereignty.

A Chinese idiom may help capture the role of the DSR for the BRI: adding wings to a tiger (*ru hu tian yi*) which means to add more capacity to strong power. Therefore, the DSR will not only benefit BRI countries, but will also serve as a flagship in the high-tech led digital transformation and globalization process in this coming digital age.

Received / Поступила в редакцию: 08.03.2022

Revised / Доработана после рецензирования: 09.04.2022

Accepted / Принята к публикации: 18.04.2022

References / Библиографический список

- Aaronson, S., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law*, 21(2), 245—272. <https://doi.org/10.1093/jiel/jgy019>
- Brynjolfsson, E., & Kahin, B. (2000). *Understanding the digital economy: Data, tools, and research*. Cambridge: MIT Press.
- Bukht, R., & Heeks, R. (2018). Defining, conceptualizing and measuring the digital economy. *International Organizations Research Journal*, 13(2), 143—172. (In Russian). <https://doi.org/10.17323/1996-7845-2018-02-07>
- Degterev, D. A., Ramich, M. S., & Piskunov, D. A. (2021). U.S. & China approaches to global Internet governance: “New bipolarity” in terms of “the network society”. *International Organisations Research Journal*, 16(3), 7—33. <https://doi.org/10.17323/1996-7845-2021-03-01>
- Degterev, D. A., Ramich, M. S., & Tsyvk, A. V. (2021). U.S. — China: “Power transition” and the outlines of “conflict bipolarity”. *Vestnik RUDN. International Relations*, 21(2), 210—231. <https://doi.org/10.22363/2313-0660-2021-21-2-210-231>
- Ding, C., Liu, C., Zheng, C., & Li, F. (2022). Digital economy, technological innovation and high-quality economic development: Based on spatial effect and mediation effect. *Sustainability*, 14(1), 1—21. <https://doi.org/10.3390/su14010216>
- Eckhardt, J., & Wang, H. Y. (2021). China’s new generation trade agreements: Importing rules to lock in domestic reform? *Regulation & Governance*, 15(3), 581—597. <https://doi.org/10.1111/rego.12258>
- Gao, H. (2021). Data regulation in trade agreements: Different models and options ahead. In M. Smeets (Ed.), *Adapting to the digital trade era: Challenges and opportunities* (pp. 323—335). Geneva: World Trade Organization.
- Gong, S., & Li, B. Q. (2019). The Digital Silk Road and the Sustainable Development Goals. *IDS Bulletin*, 50(4), 23—47. <https://doi.org/10.19088/1968-2019.137>

- Hillman, J. (2021). *The Digital Silk Road: China's quest to wire the world and win the future*. New York: Harper Business.
- Hong, Y., & Harwit, E. (2020). China's globalizing internet: History, power, and governance. *Chinese Journal of Communication*, 13(1), 1—7. <https://doi.org/10.1080/17544750.2020.1722903>
- Jiang, Y., Zhang, L., & Jin, Y. (2021). China's e-commerce development and policy relevance. In M. Smeets (Ed.), *Adapting to the digital trade era: Challenges and opportunities* (pp. 140—153). Geneva: World Trade Organization.
- Johnston, L. (2021). World trade, e-commerce, and COVID-19: Role of and implications for China's electronic World Trade Platform (eWTP). *China Review*, 21(2), 65—86.
- Joseph, R. (2001). Understanding the digital divide. *Prometheus*, 19(4), 333—336. <https://doi.org/10.1080/08109020110091396>
- Kassenova, N., & Duprey, B. (2021). *Digital Silk Road in Central Asia: Present and future*. Davis: Davis Center for Russian and Eurasian Studies.
- Lane, N. (1999). Advancing the digital economy into the 21st century. *Information Systems Frontiers*, 1(3), 317—320. <https://doi.org/10.1023/A:1010010630396>
- Lim, A. H. (2021). Trade rules for industry 4.0: Why the technical barriers to trade agreement matters even more. In S. Peng, C.-F. Lin & T. Streinz (Eds.), *Artificial intelligence and international economic law: Disruption, regulation, and reconfiguration* (pp. 97—120). Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781108954006.006>
- Liu, A., Osewe, M., Shi, Y., Zhen, X., & Wu, Y. (2022). Cross-border e-commerce development and challenges in China: A systematic literature review. *Journal of Theoretical and Applied Electronic Commerce Research*, 17(1), 69—88. <https://doi.org/10.3390/jtaer17010004>
- Luo, Y. (2022). Illusions of techno-nationalism. *Journal of International Business Studies*, (53), 1—18. <https://doi.org/10.1057/s41267-021-00468-5>
- Lv, Z., Li, X., Wang, W., Zhang, B., Hu, J., et al. (2018). Government affairs service platform for smart city. *Future Generation Computer Systems*, 81, 443—451. <https://doi.org/10.1016/j.future.2017.08.047>
- Mueller, M. L. (2020). Against sovereignty in cyberspace. *International Studies Review*, 22(4), 779—801. <https://doi.org/10.1093/isr/viz044>
- Sidorenko, E. L., & von Arx, P. (2020). Transformation of law in the context of digitalization: Defining the correct priorities. *Digital Law Journal*, 1(1), 24—38. <https://doi.org/10.38044/DLJ-2020-1-1-24-38>
- Smeets, M. (Ed.). (2021). *Adapting to the digital trade era: Challenges and opportunities*. Geneva: World Trade Organization.
- Tapscott, D. (1996). *The digital economy: Promise and peril in the age of networked intelligence*. New York: McGraw-Hill.
- Tugendhat, H., & Voo, J. (2021). China's Digital Silk Road in Africa and the future of Internet governance. Working Paper, (50), 1—25. China Africa Research Initiative, School of Advanced International Studies, Washington, DC: Johns Hopkins University. Retrieved from <https://static1.squarespace.com/static/5652847de4b033f56d2bdc29/t/61084a3238e7ff4b666b9ffe/1627933235832/WP+50+-+Tugendhat+and+Voo+-+China+Digital+Silk+Road+Africa.pdf>
- Wang, L., Zhai, Y., Wang, X., Li, J., Yuan, S., et al. (2019). Construction of telemedicine service system along the Belt and Road. *Strategic Study of Chinese Academy of Engineering*, 21(4), 1—7. <https://doi.org/10.15302/J-SSCAE-2019.04.016>
- Wang, Q., Su, M., Zhang, M., & Li, R. (2021). Integrating digital technologies and public health to fight COVID-19 pandemic: Key technologies, applications, challenges and outlook of digital healthcare. *International Journal of Environmental Research and Public Health*, 18(11), 1—50. <https://doi.org/10.3390/ijerph18116053>
- Xu, X., & Han, L. (2021). Digital economy, industrial structure upgrade and economic high-quality development: An empirical research based on the mediation effect model. *Preprints*, 1—19. Retrieved from <https://www.preprints.org/manuscript/202106.0359/v1>
- Ye, Q. (2021). Comments. In M. Smeets (Ed.), *Adapting to the digital trade era: Challenges and opportunities* (pp. 154—157). Geneva: World Trade Organization.

About the author: *Cheng Guo* — PhD (History), Post-graduate Student, Department of Political Analysis and Management, People's Friendship University of Russia (RUDN University); ORCID: 0000-0003-4927-6596; e-mail: ivanc25@yahoo.com

Сведения об авторе: *Чэн Го* — кандидат исторических наук, аспирант кафедры политического анализа и управления Российского университета дружбы народов; ORCID: 0000-0003-4927-6596; e-mail: ivanc25@yahoo.com



DOI: 10.22363/2313-0660-2022-22-2-288-302

Research article / Научная статья

Malicious Use of Artificial Intelligence in Sub-Saharan Africa: Challenges for Pan-African Cybersecurity

Konstantin A. Pantserev  

St. Petersburg State University, Saint Petersburg, Russian Federation

 pantserev@yandex.ru

Abstract. For almost two decades, Sub-Saharan African countries have been making significant efforts to ensure the rapid development of industries related to information and communication technology (ICTs) in the region. At present, all leading nations are placing greater emphasis on the development of hybrid intelligent systems capable of solving extremely complicated tasks. This includes Sub-Saharan African countries, which consider the development of advanced technologies to be an effective instrument for ensuring sustainable social and economic growth and solving a great number of the continent's problems. It has become evident, however, that all technological novelties that should simplify our lives can be used for malicious purposes. The present study examines existing practices and risks of malicious use of artificial intelligence (MUAI) in Sub-Saharan African countries. At the end of the study, the author comes to the conclusion that the problem of ensuring information, psychological, and cybersecurity is common to all African countries, which creates a serious obstacle for their further sustainable social and economic development. Over the past decade, Sub-Saharan Africa has made significant efforts to elaborate a joint vision for counteracting cybercrimes and the malicious use of advanced technologies. But all the attempts to establish effective supranational instruments that would regulate the fight against cyberattacks at the Pan-African level and take into account the interests of the vast majority of African countries in this area have failed. This demonstrates the presence of serious contradictions among African countries, which, taken together, prevent the establishment of mutually beneficial cooperation even in such an important field as cybersecurity. However, until such cooperation is established, it seems unlikely that African countries will even come close to solving this problem, which means that their information space will continue to be subjected to large-scale cyber-attacks that pose a serious threat not only to the security of individuals, but also to national and Pan-African security.

Key words: artificial intelligence, strategic communication, psychological warfare, information security, cybersecurity, Sub-Saharan African countries

Acknowledgements: This research was supported by the St. Petersburg State University, project No. 93024916 “Artificial Intelligence and Data Science: Theory, Technology, Sectoral and Interdisciplinary Researches and Applications”.

© Pantserev K.A., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

For citation: Pantserev, K. A. (2022). Malicious use of artificial intelligence in Sub-Saharan Africa: Challenges for Pan-African cybersecurity. *Vestnik RUDN. International Relations*, 22(2), 288—302. <https://doi.org/10.22363/2313-0660-2022-22-2-288-302>

Злонамеренное использование технологий искусственного интеллекта в странах Африки южнее Сахары: вызовы panaфриканской кибербезопасности

К.А. Панцеров  

Санкт-Петербургский государственный университет, Санкт-Петербург, Российская Федерация
 pantserev@yandex.ru

Аннотация. На протяжении двух десятилетий страны Африки южнее Сахары прилагали значительные усилия, направленные на быстрое развитие информационно-коммуникационных технологий. В настоящее время все ведущие мировые державы уделяют повышенное внимание созданию гибридных интеллектуальных систем, способных решать наиболее сложные задачи. Страны Африки южнее Сахары не остались в стороне от этого процесса. Их правительства убеждены, что передовые технологии являются наиболее эффективным инструментом, способным обеспечить устойчивый социально-экономический рост и решить наиболее насущные проблемы. Однако любые технологические новации, которые призваны упростить нашу жизнь, могут быть использованы и в злонамеренных целях. Настоящее исследование показывает возможные риски злонамеренного использования технологий искусственного интеллекта в странах Африки, расположенных южнее Сахары. Некоторые из этих рисков уже стали реальностью. Автор приходит к выводу, что проблема обеспечения информационно-психологической и кибербезопасности является общей для всех африканских стран. Именно она встает на пути обеспечения дальнейшего устойчивого социально-экономического роста государств рассматриваемого региона. На протяжении последнего десятилетия страны Африки южнее Сахары старались выработать совместное видение борьбы с киберпреступлениями и злонамеренным применением передовых технологий. Однако все их попытки создать действенные наднациональные институты, которые регулировали бы борьбу с кибератаками на panaфриканском уровне и учитывали бы интересы подавляющего большинства африканских стран, провалились. Данное обстоятельство демонстрирует наличие серьезных противоречий среди африканских государств, которые препятствуют установлению взаимовыгодного сотрудничества даже в такой важной сфере, какой является проблема обеспечения кибербезопасности. Тем не менее пока подобное сотрудничество не будет налажено, представляется маловероятным, что африканские страны хотя бы приблизятся к решению данной проблемы, что означает, что они и в дальнейшем будут подвергаться масштабным кибератакам, которые создают серьезную угрозу для личной, национальной и panaфриканской безопасности.

Ключевые слова: искусственный интеллект, стратегическая коммуникация, информационно-психологическое противоборство, информационная безопасность, кибербезопасность, страны Африки южнее Сахары

Благодарности: Статья выполнена при финансовой поддержке СПбГУ, проект № 93024916 «Искусственный интеллект и наука о данных: теория, технология, отраслевые и междисциплинарные исследования и приложения».

Для цитирования: Панцеров К. А. Злонамеренное использование технологий искусственного интеллекта в странах Африки южнее Сахары: вызовы panaфриканской кибербезопасности // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 288—302. <https://doi.org/10.22363/2313-0660-2022-22-2-288-302>

Introduction

Sub-Saharan African countries have become a subject “of global interest with

regards to technological development, leapfrogging and foreign investment, despite the lag in socio-economic development in

comparison with other regions” (Haula & Agbozo, 2020). All leading powers are currently paying increasing attention to research aimed at the creation of hybrid intelligent systems that can solve very complicated tasks. Thus includes the nations of Sub-Saharan Africa, which consider the development of advanced technologies to be an effective instrument for ensuring sustainable social and economic growth and solving many of the problems in the region. It has become evident, however, that all technological novelties that should simplify daily life can be used for malicious intent.

The use of artificial intelligence (AI)-based technologies opens a wide range of possibilities for hackers and provides the possibility for them to go through any cyber defense. Thanks to advanced technologies, hackers can:

- hide malicious codes in official, secure applications;
- affect voice or visual authentication;
- put devices under their control through the use of private keys;
- organize intelligent attacks over systems or networks;
- simulate reliable system components.

With this in mind, the following hypothesis is proposed: any AI technologies can be applied either usefully or maliciously, and it is just a matter of time before all types of criminals become familiar with them. While states should support the development of advanced technologies, they should also ensure that governmental bodies, society, and individuals are not harmed by the misuse of such technologies.

Two main methods are used in this paper: case studies of the level of development in advanced technologies in different Sub-Saharan African countries and critical discourse analysis of different national strategies, road maps, and so on, devoted to the further development and implementation of AI technologies in Africa and ensuring the

cybersecurity of African countries. This method was chosen because critical discourse analysis, as a method, “shows how language works in sociocultural and political contexts, focusing on power relations and ideological perspectives reflected in discourse texts, and their wider implications for the society” (Chiluwa, 2019b). It therefore helps in identifying “social problems expressed or reflected in texts (such as political power abuse, racial discrimination, xenophobia, or terror threats) as one of its main objectives and the possibility of finding solutions to them” (Chiluwa, 2019b).

Using analyses of the existing AI technology initiatives in Sub-Saharan Africa, the paper reveals the most obvious prospective threats. Three questions form the core of the research: What is the current level of development of AI technologies in Africa? Has AI already been used maliciously in Sub-Saharan Africa? What measures should Sub-Saharan African countries undertake to stop the further malicious use of advanced technologies? The author concludes by suggesting the measures necessary for strengthening the information and psychological security of Sub-Saharan African countries.

Literature Review

The current scientific discourse includes a wide range of articles on different aspects of AI,¹ some of which focus on its malicious use

¹ See: Chandler S. Deepfakes 2.0: The Terrifying Future of AI and Fake News // Daily Dot. October 5, 2018. URL: <https://www.dailydot.com/debug/deepfakes-ai-clones-fake-news> (accessed: 04.07.2021); Chesney R., Citron D. Deepfakes and the New Disinformation War: The Coming Age of Post Truth Geopolitics // Foreign Affairs. January/February 2019. URL: <https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war> (accessed: 04.07.2021); Fillion R. M. Fighting the Reality of Deepfakes // Nieman Lab. 2019. URL: <https://www.niemanlab.org/2018/12/fighting-the-reality-of-deepfakes> (accessed: 30.07.2021).

(e.g., Brundage et al., 2018; Chesney & Citron, 2018; Antinori, 2019; Bazarkina & Pashentsev, 2019; Dack, 2019), while other are devoted to different issues involved in psychological warfare in general and the manipulation of information in particular (e.g., Jeangène Vilmer et al., 2018; Pashentsev, 2019; Bazarkina, Pashentsev & Simons, 2020). There is a lack of research on the development of AI in Sub-Saharan Africa, including the extent to which countries in the region are protected from potential and actual malevolent application of such advanced technologies. The present article intends to fill this gap.

Advanced Technologies in Sub-Saharan Africa: Myth or Reality

The necessity of the development of advanced technologies is considering as the essential condition for the ensuring of the world leadership in the contemporary world. According to Haula and Agbozo (2020), at first glance it appears that African countries face a large number of non-technical problems, such as “civil unrest, corrupt governance, low educational enrolment levels, poor healthcare delivery, a wide digital divide, as well as lacking infrastructure to meet present day global socio-economic demands.” It would seem that the need for AI development must inevitably take a back seat; however, this is not quite true: “Within the past decade, there have been massive shifts in the realization of the role of technology and innovation in contributing to the alleviation of the woes of the sub-region” (Haula & Agbozo, 2020).

African countries see the development of breakthrough technologies as a certain guarantee of their technological sovereignty and are convinced that AI technologies could solve many of the continent’s traditional problems, among others (Artificial Intelligence for Africa..., 2018).

Thus, in agriculture AI technologies could be used to improve productivity and increase

the efficiency of agricultural work. The unmanned aerial vehicles equipped with hybrid intelligence systems could be widely applied in Africa. These drones could be used not only for fertilizing agricultural plantations, but also be equipped with precise sensors that would help in aerial monitoring to detect signs of pests and crop diseases, as well as assess the extent of soil aridity and weed damage. The images obtained from the drones would then be automatically checked and analyzed together with other available data and provide farmers with valuable information about the health of their crops without the need for additional laboratory studies.²

AI technologies could also provide significant assistance in the modernization of the health-care systems of African countries, making medicine in the region more high-tech. One of the main problems of African medical institutions is the lack of qualified medical personnel, and AI technologies could partially solve this problem by providing primary medical diagnostics, and collecting and processing data about the patients and their medical history. The doctor would then be able to receive more patients in one shift. Advanced technologies could also increase the level of medical diagnostics and detect dangerous diseases at an earlier stage, which increase the chance of full recovery. AI would also be useful in providing remote diagnostics to rural areas via chatbots and computer vision, thus providing access to millions of Africans who would not otherwise be able to access medical care. Thus, chatbots, for example, “may minimize hospital visits and assist with triaging before medical consultation. Specially designed AI mobile applications requiring little skills can help in diagnosing birth asphyxia and malaria in the rural areas of Africa where there is a shortage

² Oduma E. How AI Can Transform Kenyan Industries // Ai Kenya. January 21, 2019. URL: <https://kenya.ai/how-ai-can-transform-kenyan-industries> (accessed: 28.07.2021).

of skilled health workers and medical equipment” (Owoyemi et. al., 2020).

AI could also be widely used by African governments and significantly reduce paperwork, improve public sector the efficiency, and speed of public service delivery. This would allow the heads of governmental bodies to solve the problem of resource allocation by redirecting staff where they would be most useful. The predictive capabilities of AI may be of particular importance, as these would allow government officials and policymakers to respond more quickly to societal needs: from preventive intervention by social services to help children and other socially vulnerable segments of the population in difficult life situations, to crime prevention and rapid response in emergencies. Finally, AI-based algorithms could provide citizens with new platforms for assessing the quality, adequacy, and effectiveness of public services, which would provide more effective feedback to the population.

Hybrid intelligence systems could also be used in education to automate the assessments, which would allow teachers to free up time for other important tasks, including additional counseling for students on the subjects studied, preparing for classes, or improving their own skills. AI could also provide additional support to students and offer help with automated tutors and curators to create an individual learning trajectory based on the abilities of each individual student. AI could also be used to monitor student performance and alert teachers of possible academic performance issues, providing useful feedback on course effectiveness.

In this respect, AI is a powerful potential tool to help African countries tackle the continent’s most significant challenges and ensure their sustainable socio-economic growth and transition to an innovation economy. And African countries themselves are striving to conduct their own scientific research in the

field. Thus, a number of startups using technical solutions in the field of AI are already being implemented.

In South Africa, for example, a special data management service called MySmartFarm was launched on 1 June 2012, “which simplifies technology for farmers frustrated by the collection and interpretation of information from multiple sources. It automatically collects all kinds of data and aggregates it with easy-to-use farm management tools’ data, in order to present usable information, advice and predictions for each field on easy to use dashboards and mobile Apps.”³ This start-up quickly became in great demand among South Africans and in 2013 has won IBM’s South Africa SmartCamp award, which supposed support and mentorship from IBM.⁴

Another start-up, the *DroneClouds*, was launched in South Africa in 2015. It “helps farmers increase yield by giving them to-the-point, actionable crop insights using drones, satellite, mobile, the cloud and agro experts.”⁵

In Ghana the start-up *SyeComp* “focuses on enhancing agriculture through ICT and advanced geospatial solutions, research and knowledge management. It specializes in the acquisition, processing, analysis and synthesis of geospatial data from satellites and multispectral drone sensors for various applications using geographic information systems (GIS) and remote sensing (RS) technology. *SyeComp* provides support for various actors across and along the value chains in new dynamics of gathering multispectral and hyperspectral image data and

³ MySmartFarm // Solar Impulse Foundation. URL: <https://solarimpulse.com/companies/mysmartfarm> (accessed: 18.08.2021).

⁴ Sanchez D. MySmartFarm Ag Solution Wins IBM SmartCamp Award // The Moguldom Nation. October 11, 2013. URL: <https://moguldom.com/24914/mysmartfarm-app-wins-ibm-south-africa-award> (accessed: 01.02.2022).

⁵ Lourie G. 7 South African Drone Firms to Keep an Eye on // TFS Media. September 12, 2017. URL: <https://www.techfinancials.co.za/2017/09/12/httpstalkiot-co-za201709117-south-african-drone-firms-to-keep-an-eye-on> (accessed: 01.02.2022).

disseminating information through multiple channels to gain relevant insights” (Artificial Intelligence for Africa..., 2018, p. 19).

Kenya also started implementing two startups based on AI-algorithms. One of them, called *FarmDrive*, represents a technological platform, that provides financial institutions with a model, based on a large amount of data, relevant to the agricultural industry, necessary for risk assessment when issuing loans and developing targeted loan products that would meet the needs of small farmers.⁶ Another start-up supposes integration into social networks and messengers of a specialized chatbot named *Sophie*.⁷ This free chatbot, equipped with a convenient voice interface, represents a platform on which any user can ask questions in the intimate sphere, including in the field of reproductive medicine, and get an exhaustive answer. This service is available in several popular social media platforms, such as Messenger and Twitter.

Nigeria is also actively implementing AI technologies into people’s daily life. The most successful example is the technological platform *Kudi.ai* (“kudi” means money in the Hausa language). It was launched in 2017 and represents a chatbot functioning on AI algorithms; its main task is to provide assistance in the financial sphere, including transferring money and paying bills. Also, as in the case chatbot of Sophie, Kudi is integrated into most popular messaging apps and social networks, in particular, Facebook (On March 21, 2022, the Tverskoy District Court of Moscow satisfied the claim of the Prosecutor General’s Office of the Russian Federation and recognized the activities of the social networks Instagram and Facebook, owned by Meta, as extremist, banning their work in Russia. — *Editor’s note*).⁸ Another chatbot, called *Lara*,

launched on March 5, 2017, is an intelligent system that helps users get from one point to another by providing detailed text, step-by-step instructions, and determining the exact fare in advance.⁹

Nigeria’s banking sector is also starting to use AI-technologies. Thus, located in Nigeria, *Zenith Bank* “launched several new solutions that enable more convenient, safe and quick customer transactions. These include the bank’s Scan to Pay App which can be used by Zenith and non-zenith customers to make online and in-store payments in seconds through quick response code scanning on any internet enabled phone. The bank’s mobile app also offers enhanced functionalities such as instant account opening for new customer” (Artificial Intelligence for Africa..., 2018, p. 14).

And in May 2017 another Nigerian Bank — the Wema Bank — launched the first African fully digital Bank called the ALAT. It gives the opportunity for customers to “open an account via mobile phone or Internet in under five minutes and debit cards are delivered anywhere in Nigeria within two to three days, free of charge” (Artificial Intelligence for Africa..., 2018, p. 14).

In Uganda there has been launched the *Awamo* — “a digital banking platform and credit bureau that uses AI to reduce fraud when signing up customers and businesses to its platform. The platform helps digitise business procedures, credit information sharing, and many other services using mobile devices” (Butcher, Wilson-Strydom & Baijnath, 2021, p. 48).

Based on all these examples, we can conclude that African countries are beginning to use AI technology in the creation of various services aimed at meeting the needs of their

⁶ FarmDrive. URL: <https://farmdrive.co.ke> (accessed: 18.08.2021).

⁷ SophieBot. URL: <https://web.archive.org/web/20161104205907/http://www.sophiebot.tk/> (accessed: 18.08.2021).

⁸ Akinwamide N. Kudi AI is Putting a Human Feel to Online Payments in Nigeria // Techpoint Africa. February

8, 2017. URL: <https://techpoint.africa/2017/02/08/kudi-ai-online-payments-nigeria> (accessed: 29.07.2021).

⁹ Ndiomewese I. Startup Profile: Lara — Get Step-By-Step Public Transportation Directions to Any Destination // Techpoint Africa. April 17, 2017. URL: <https://techpoint.africa/2017/04/17/lara-profile> (accessed: 29.07.2021).

citizens. But at the same time, it must be remembered that all these technologies can be used maliciously. That's why it seems extremely important to examine existing practices and risks of malicious use of artificial intelligence (MUAI) in Africa.

Risks of Malicious Use of AI in Sub-Saharan Africa

Sub-Saharan African countries are already suffering cyberattacks of a different kind, such as phishing, DDoS-attacks, and data theft (Interpol, 2020). The last point leads us to the conclusion that when developing the ICT sector in a particular country, it is necessary to think about ensuring the information security of the whole country and its citizens.

According to official data in 2017, the total loss due to cybercrime across Africa amounted to 3.5 billion USD. The largest amount of damage, 649 million USD, was caused to Nigeria, Kenya keeps the second place, with 210 million USD, and South Africa rounds out the top three with a total of 157 million USD in damages.¹⁰ Undoubtedly these impressive figures underscore the fact that African governments must do something to strengthen information security in their countries. A further analysis of the statistics indicates that African banks are most vulnerable to cyberattacks, as they are the focus of 23% of attacks, followed by government bodies at different levels (19%), ecommerce (16%), mobile-based transactions (13%) and telecommunication (11%).¹¹

The problem is complicated by the fact that Africa's digital infrastructure is rather ill-equipped to manage the continent's growing

cybersecurity risk, and more than 60% of African enterprises have not trained their staff in the field of cybersecurity. More than 90% of big African companies spend less than 10,000 USD on different cybersecurity issues and are operating below the cybersecurity poverty level.¹² Thus, African countries are very attractive to any kind of cybercriminal. A 2013 report on whether Africa is a safe harbor for cybercriminals highlights two key circumstances that contribute to the growth of cybercrime in Africa: mass access to the fiber-optic broadband communication system, which contributes to a rapid increase in the number of Internet users, and the lack of developed legislation in the field of cybersecurity (Kharouni, 2013). At the same time, although a number of African countries have adopted laws aimed at protecting personal data and combating cybercrime in recent years, there have been no positive changes in this area, and, indeed, a sharp increase in the number of cybercrimes in Africa poses a serious threat to personal, national, and even international psychological security.

Although Sub-Saharan African countries have an increased focus on advanced technology, "they seldom have national strategies to support future plans. At present, high levels of corruption in public institutions and weak data infrastructure that is susceptible to data leaks pose a threat to data privacy and successful AI implementation" (Butcher, Wilson-Strydom & Bajinath, 2021, p. 62).

The vast majority of cybercrime offences committed in Africa are financial in nature and target individuals for theft. According to Interpol's African Cyberthreat Assessment Report, the following major cyberthreats can be highlighted for Africa: online scams, digital extortion, business e-mail compromise, botnets, and ransomware.¹³

¹² Ibid.

¹³ Cyberthreat Assessment Report: Interpol's Key Insight into Cybercrime in Africa // Interpol. October 21, 2021. URL: <https://www.interpol.int/News-and-Events/>

¹⁰ Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line // Serianu. 2017. URL: <https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf> (accessed: 05.07.2021).

¹¹ Isiavwe D. Cybersecurity Threat Evolution: Perspectives from Africa // The Information Security Society of Africa — Nigeria. February 15, 2020. URL: <https://www.issan.org.ng/download/cyber-security-threat-evolution> (accessed: 05.07.2021).

The situation is simplified by the fact that mass digitalization has created a great number of different databases with personal details for a huge number of ordinary people. In Africa, such databases have very poor cyber-defense and can quite often fall into the hands of intruders who use the information maliciously to get something of value from their victims.

One of the largest cyberattacks in Africa is the leakage of personal data from residents of the Republic of South Africa, which occurred in 2017.¹⁴ Files containing personal information of millions of South Africans, both living and deceased, became freely available on the Internet, including their national identity numbers, information about marital status, income, information about work and the current position, and information about their property. It is noteworthy, that this data leak cannot be called a hacker attack in the full sense, because all of this information about users was posted on the website of the data processing company Dracore Data Sciences without any additional protection.¹⁵ It is quite obvious that it was only a matter of time before this information would fall into the hands of hackers, who can now dispose of it at their discretion.

In addition to such cases, which have all the signs of criminal negligence, African countries regularly face massive cyberattacks, some of which actively use the possibilities of AI and attack critical infrastructure in Africa. Thus, *Life Healthcare*, the second largest

operator of private hospitals in South Africa responsible for the supply of digital services in hospitals throughout South Africa, faced a large-scale cyberattack in June 2020 that put its reception systems, business processing systems, and email servers out of service. This led to a month of downtime and caused fatal consequences in the midst of the coronavirus pandemic.

In October 2020, two other cyberattacks occurred in South Africa that took key social and emergency services in Johannesburg out of service: “Analysis of the attack identified not only the exploitation of a vulnerability, but also that after employing lateral movement techniques the threat actors deliberately deployed their ransomware to coincide with the end of the month payment cycle — in an effort to further coerce South African authorities to pay the cryptocurrency ransom.”¹⁶ In July 2021, the state-owned South African company Transnet faced an unprecedented cyberattack, as a result of which container operations in both major South African ports — Cape Town and Durban — were disrupted. On July 22, 2021, the official Transnet website went down and only showed an error message. The company, which operates the major ports in South Africa, as well as a huge railway network transporting minerals and other goods for export, officially confirmed that its IT infrastructure experienced failures. The Institute for Security Studies (ISS) highlighted that, for the “first time the integrity of South Africa’s critical maritime infrastructure has been severely disrupted” with an attack on the port able to delay or shut down a critical trade route and disrupt vital trade services.”¹⁷ Thus “most of the copper and cobalt mined in the Democratic Republic of Congo and Zambia, where miners such as Glencore and Barrick

News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa (accessed: 11.07.2021).

¹⁴ Mohapi T. What We Know So Far about South Africa’s Largest Ever Data Breach // iAfrikan. October 18, 2017. URL: <https://web.archive.org/web/20210122034431/https://iafrikan.com/2017/10/17/south-africas-govault-hacked-over-30-million-personal-records-leaked/> (accessed: 11.07.2021).

¹⁵ Mohapi T. Is Dracore Data Sciences Responsible for South Africa’s Largest Ever Data Leak? // iAfrikan. October 18, 2017. URL: <https://web.archive.org/web/20210404225144/https://www.iafrikan.com/2017/10/18/dracore-data-sciences/> (accessed: 11.07.2021).

¹⁶ Cyberthreat Assessment Report: Interpol’s Key Insight into Cybercrime in Africa // Interpol. October 21, 2021. URL: <https://www.interpol.int/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa> (accessed: 11.07.2021).

¹⁷ Ibid.

Gold operate, use Durban to ship cargo out of Africa.”¹⁸ This last example clearly demonstrates how advanced technologies can be used maliciously to disable critical infrastructure in African countries. The true reason for the cyberattack on the Transnet computer systems has also not been established, but there some concern that it could be related to the riots and violence that had swept through some parts of the country earlier in the year.

From time to time Ethiopia has also faced large-scaled cyberattacks on its critical infrastructure. The Nile River’s Grand Ethiopian Renaissance Dam is widely known to be a source of tension between Ethiopia and Egypt, and in June 2020, the Egypt-based actor known as the Cyber Horus Group hatched plans for a big cyberattack to create “significant economic, psychological, and political pressure on Ethiopia over the filling of the Nile River’s Grand Ethiopian Renaissance Dam (GERD).”¹⁹ The group managed to hack a number of government websites and spread messages threatening war if Ethiopia began filling the dam.

The last example illustrates that sometimes advanced technologies are used in Africa to manipulate public opinion and increase social tension. The most suitable technology for this is the creation of fake video and audio. By itself, this technology, also called ‘deepfakes,’ represents a synthesis of images using appropriate AI algorithms, that results in the apparent clone of a real person who moves and speaks just like the template. This technology opens a wide range of opportunities for malicious use and poses a

serious threat to personal, national, and international security, because it allows a hacker or a potential terrorist to make any politician or well-known person appear to say and do whatever the hacker wants, and this false video can be posted on social media platforms (on fake profiles) or on a fake website for well-known media. The fake video can quickly spread all over the web and end political careers or even cause deep political crises between nations. It is noteworthy that “convincing deepfakes can be made by pretty much anyone with the right hardware and software and a few hours to kill. The results can wreak havoc on individual livelihoods and reputations, but more frighteningly, can be used to manipulate en masse.”²⁰

One of the most revealing examples of the use of advanced technologies to incite mass discontent and tension in relations between different African countries is the active use of deepfakes during the wave of riots and violence that swept through South Africa in 2019 on the basis of xenophobic sentiments, after truck drivers staged a strike in protest against the employment of foreigners. During the mass pogroms of foreign-owned enterprises in Johannesburg in early September 2019 twelve people were killed. Although nobody from Nigeria has actually been suffered (among those killed ten were South African citizens and two were Zimbabweans), a number of fake videos and images that allegedly depicted attacks and murders of Nigerians or their mass deportation rapidly appeared on social media.²¹ To further incite mass discontent, a video taken out of context also appeared on online that claims to depict a

¹⁸ Shabalala Z., Heiberg T. Cyber Attack Disrupts Major South African Port Operations // Reuters. July 22, 2021. URL: <https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/> (accessed: 29.09.2021).

¹⁹ Allen N. Africa’s Evolving Cyber Threats // Africa Center for Strategic Studies. January 19, 2021. URL: <https://africacenter.org/spotlight/Africa-evolving-cyber-threats> (accessed: 29.09.2021).

²⁰ Neille D. Manipulating Reality: The Rise of Deepfakes and How to Spot Them // Daily Maverick. May 05, 2021. URL: <https://www.dailymaverick.co.za/article/2021-05-05-manipulating-reality-the-rise-of-deepfakes-and-how-to-spot-them> (accessed: 18.09.2021).

²¹ Faife C. In Africa, Fear of State Violence Informs Deepfake Threat // WITNESS. December 9, 2019. URL: <https://blog.witness.org/2019/12/africa-fear-state-violence-informs-deepfake-threat> (accessed: 18.07.2021).

burning building in South Africa, although the fire was actually located in India in the state of Gujarat.²² As a result of these deepfakes, Nigeria withdrew a delegation from a big international conference held in South Africa and announced the evacuation of its citizens from that country. This forced South Africa to make an official apology to Nigeria for the xenophobic attacks that caused a surge in tension between two countries, and to assure its Nigerian partners that all cases of mass pogroms of Nigerian-owned enterprises would be thoroughly investigated.²³ This type of malicious use of advanced technologies to incite conflict between two countries in a region where many countries have unresolved disputes and claims against each other poses a very serious threat to international information and psychological security, because any such clash could escalate into another full-scale armed conflict.

It might also intensify the activity of different terrorist groups on the continent, such as Boko Haram in Nigeria, Ansar al-Din in Mali, Movement for Unity and Jihad in West Africa, and Al-Shabaab in Somalia. These groups could start using advanced technologies to improve communications between fighters, spread propaganda their views throughout Africa, and recruit new supporters: “Because the Internet combines the advantages of speed, cheapness, accessibility, and anonymity, it offers terrorists a variety of media options to sell their extremist ideology and message and attempt to radicalize other Internet users who may have sympathy for them” (Chiluwa, 2019c, p. 208). The Internet in general — and

²² Burning Building Video from India, Not from Xenophobic Violence in South Africa // Africa Check. September 19, 2019. URL: <https://africacheck.org/fact-checks/fbchecks/burning-building-video-india-not-xenophobic-violence-south-africa> (accessed: 18.07.2021).

²³ South Africa Offers ‘Profuse’ Apologies to Nigeria After Attacks // Al Jazeera. September 16, 2019. URL: <https://www.aljazeera.com/news/2019/9/16/south-africa-offers-profuse-apologies-to-nigeria-after-attacks> (accessed: 18.07.2021).

social media in particular — should be considered as a very dangerous instrument for terrorist propaganda and recruitment (Chiluwa, 2019a, p. 522). As Ishengoma has argued, “The prominence of Internet communications in contemporary social life and the application of the Internet and ICT to advance terrorist activities have given rise to the concept of ‘Terrorism 2.0,’ where terrorist groups have extensively adopted web 2.0 applications and semantic technology tools to propagate their activities” (Ishengoma, 2013).

It is just a matter of time before terrorists become familiar enough with AI and start using its possibilities to organize high-tech terroristic attacks. Boko Haram, for example, is actively using surveillance drones, which are “reportedly more sophisticated than those used by the government.”²⁴ Al-Shabaab “already has been accused of ‘twitter terrorism,’ and hate-speech warranting the shutting down of their Twitter accounts at different times” (Chiluwa, Chimunya & Ajiboye, 2020). African countries should therefore focus all their efforts on strengthening their information, psychological, and cyber security and prevent further malicious use of AI-based technologies.

Ensuring Psychological Security in Sub-Saharan Africa: Challenges and Prospects

The issue of information, cyber and psychological security remains one of the key issues hindering the further sustainable socio-economic development of sub-Saharan Africa. According to Allen, “the continent faces a growing 100,000-person gap in certified cybersecurity professionals.”²⁵ Many organizations, businesses, and agencies lack basic cyber awareness and fail

²⁴ Allen N. Africa’s Evolving Cyber Threats // Africa Center for Strategic Studies. January 19, 2021. URL: <https://africacenter.org/spotlight/Africa-evolving-cyber-threats> (accessed: 29.09.2021).

²⁵ Ibid.

to implement rudimentary cybersecurity measures. Governments frequently fail to monitor threats, collect digital forensic evidence, and prosecute computer-based crime. 96% of cyber security incidents go unreported or unresolved, meaning that cyber threats in Africa are likely much worse than recognized.²⁶ A number of African countries are, however, working hard on this issue and have initiated the significant modernization of relevant national legislature, because “for states with weaker cyber security capacities, a strong legal and normative framework is an essential element affording protection from foreign interference and cyber threats.”²⁷ According to data provided by the International Telecommunication Union (ITU), about 40 African countries have cybercriminal legislation and cybersecurity regulations in place. Moreover, eleven countries — South Africa, Botswana, Uganda, Zambia, Burkina Faso, Tanzania, Cameroon, Nigeria, Benin, Ghana and Côte d’Ivoire — have developed complex commitments and engage in cybersecurity programs and initiatives.²⁸

Rwanda, Kenya, and Uganda, for example, have undertaken a number of measures to counteract cyberthreats and protect data in cyberspace. These measures should be recognized as effective, but they are not sufficient for a comprehensive solution to the problem. Rwanda, for example, has elaborated a National Policy on the field of cyber security, which supported the creation of the National Center of Computer Security and Response

²⁶ Van der Waag-Cowling N. Living Below the Cyber Poverty Line: Strategic Challenges for Africa // Humanitarian Law and Policy. June 11, 2020. URL: <https://blogs.icrc.org/law-and-policy/2020/06/11/cyber-poverty-line-africa> (accessed: 18.08.2021).

²⁷ Ibid.

²⁸ Digital Trends in Africa: Information and Communication Technology Trends and Developments in the Africa Region, 2017—2020 // International Telecommunication Union, 2021. URL: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_AFR.01-2021-PDF-E.pdf (accessed: 18.08.2021).

focused on the identification and prevention of cyberthreats. The National Cyberspace Emergency Plan to counteract cyber crises has also been elaborated. Finally, a law on ICT in Rwanda was adopted in 2016 that contains a number of articles devoted to the malicious use of information technologies for the purpose of committing crimes which imposes criminal liability for unauthorized access to data.²⁹

Kenya elaborated its own National Cyber Security Strategy in 2014.³⁰ Following this strategy, amendments have been adopted to the law on ICT aimed at the criminalization of illegal access to information. The National Kenya Computer Incident Response Team — Coordination Centre (National KE-CIRT/CC) has also been created, which is supported by the ITU to coordinate responses to cybersecurity matters at the national level in collaboration with relevant actors both locally and internationally.³¹

Uganda also has a more or less well developed legislative base for ensuring cybersecurity. The country has adopted a special law on the malicious use of computers, which ensures the protection of wire transactions and makes it possible to monitor and intercept suspicious messages. A special National Cyberspace Emergency Response Team and a specialized National Information

²⁹ Rwanda: 2016 Law Governing Information and Communication Technologies // ARTICLE 19. May 2018. URL: <https://www.article19.org/wp-content/uploads/2018/05/Analysis-Rwanda-ICT-Law-April-2018.pdf> (accessed: 18.08.2021).

³⁰ National Cybersecurity Strategy of Kenya // Ministry of Information Communications and Technology of Kenya. February 2014. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Kenya_2014_GOK-national-cybersecurity-strategy.pdf (accessed: 18.08.2021).

³¹ Digital Trends in Africa: Information and Communication Technology Trends and Developments in the Africa Region, 2017—2020 // International Telecommunication Union. 2021. URL: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_AFR.01-2021-PDF-E.pdf (accessed: 18.08.2021).

Advisory and Technology Body have also been created, whose tasks include providing technical support and training in the field of cybersecurity.

It is impossible to solve all of the challenges facing African countries in this area only through the introduction of various prohibitive measures at the national level. The problem of ensuring cyber and psychological security is complicated, and a comprehensive solution is possible only through the involvement of all stakeholders, which include representatives of various governmental bodies, top managers of big companies, representatives of the financial sector, and civil society.

At the same time, special emphasis should be placed on the need to intensify cooperation in this area among all African countries. For this purpose, the African Information Security Association (AISA) was created in 2006 as the result of the *International Conference on Computer Security and Cybercrime in Africa*.³² AISA's mission is to develop information security in Africa, and any stakeholder concerned about ensuring information security — including individuals, organizations, and various governmental bodies — can join the association. According to the information provided on the website, AISA's main activity is aimed at sharing world best practices in the field of information, computer, and Internet security and organizing campaigns to combat cybercrime in Africa, primarily by organizing and holding seminars and conferences, publishing books, and magazines, and maintaining websites and blogs, as well as developing various security guidelines and consultations.³³ The annual monitoring of the level of information security in Africa is one of AISA's most important activity streams. Despite more

³² African Information Security Association (AISA). URL: <https://web.archive.org/web/20120128191125/http://www.jidaw.com/aisa> (accessed: 18.08.2021).

³³ Ibid.

than a decade of work, we have not been able to find any meaningful results from its activities, and the content of its website remains very poor.

Among other important initiatives demonstrating the attempt of African countries to develop a joint approach to ensuring information security there should be noted the African Union *Convention on Cyber Security and Personal Data Protection*, which was adopted in 2014 in Malabo, Equatorial Guinea.³⁴ The appearance of this document should be considered an important step that proves the desire of African countries to develop joint mechanisms to further combat cybercrime and “provide a framework for cybersecurity in Africa. As part of this, member states are asked to establish national cybersecurity policies as well as legal, regulatory, and institutional frameworks for cybersecurity governance.”³⁵ At the same time, however, the process of signing and subsequent ratification of this document shows the existence of serious contradictions between different African countries in the field of cybersecurity. To date, the *Convention* has been signed by only 14 African countries, and only 13 have ratified it (Angola, Cape Verde, Congo, Ghana, Guinea, Mozambique, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo and Zambia).³⁶ It is noteworthy that

³⁴ African Union Convention on Cyber Security and Personal Data Protection // The Institute for Security Studies. June 27, 2014. URL: <https://issafrica.org/ctafrica/uploads/AU%20Convention%20on%20Cyber%20Security%20and%20Personal%20Data%20Protection.pdf> (accessed: 21.07.2021).

³⁵ Jili B. The Spread of Surveillance Technology in Africa Stirs Security Concerns // Africa Center for Strategic Studies. December 11, 2020. URL: <https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns> (accessed: 05.09.2021).

³⁶ List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection // African Union. March 25, 2022. URL: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf (accessed: 01.04.2022).

regional leaders in the field of ICTs, such as Kenya, Nigeria, and South Africa have not signed this document. Indeed, the *Convention* has not yet entered into force, because it must be ratified by at least 15 countries,³⁷ so it can therefore be considered only as another program document trying to regulate one of the most important areas of cooperation related to cybersecurity. But “even with the challenge in ratification, it remains a major step forward towards increasing awareness amongst the ministers and administrators from member states.”³⁸ The *Convention* again shows that supranational institutions and instruments work extremely poorly in African circumstances, perhaps because of the many contradictions among African countries, which, taken together, prevent them from developing common working tools to solve the most significant problems of the continent, including information, psychological and cybersecurity.

In this regard, only the ISSAN has managed to achieve relative success and become a real platform for cooperation and exchange of views between all stakeholders, including banks, telecommunications companies, government agencies, government regulators, IT companies, information security consultants, and lawyers.³⁹ It must be particularly emphasized that ISSAN is a non-profit organization whose objective is to ensure that Nigeria's cyberspace, primarily the banking and public sectors, is protected and the organization solves this task

³⁷ African Union Convention on Cyber Security and Personal Data Protection // African Union. June 27, 2014. URL: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed: 05.09.2021).

³⁸ Tomlin S. N. Cyberspace Security in Africa — Where Do We Stand? // African Academic Network on Internet Policy. February 12, 2020. URL: <https://aanoip.org/cyberspace-security-in-africa-where-do-we-stand> (accessed: 18.08.2021).

³⁹ Information Security Society of Africa — Nigeria (ISSAN). URL: <https://issan.org.ng> (accessed: 18.08.2021).

by carrying out a set of activities aimed at familiarizing all stakeholders with best practices in this area.

Conclusion

In conclusion, we would like to make a few important points.

Firstly, Sub-Saharan African countries are paying increased attention to the elaboration of different technological solutions based on AI algorithms. The use of unmanned aerial vehicles should be considered as the most promising technology with the great potential in the region. According to Haula and Agbozo (2020), “drone technology has the capacity to improve upon service delivery in the agriculture, health and security sectors of sub-Saharan Africa.” For example, such drones can be used for “monitoring terrorist movements and identifying targets/threats; healthcare delivery; land administration, and cadastral intelligence; fertilizer and irrigation treatments; crop performance improvement; automation of pestilence combating.”

Secondly, all new technologies can be used for malicious intent. The states of Sub-Saharan Africa continue to suffer from cyber-crimes of all kinds, which in the age of rapid development of AI-based technologies are becoming increasingly high-tech. The problem of ensuring information, psychological, and cybersecurity is common to all African countries, which creates a serious obstacle for their further sustainable social and economic development. As Vattapparamban et al. (2016) argue, when an unmanned aerial vehicle goes beyond the line of sight, it can be used as a signal sniffer. Drones also can be used for cyber-attacks, interdiction of other drones, or even GPS spoofing. Such threats should be carefully studied before the use of drones becomes widespread in the region.

Thirdly, over the past decade, Sub-Saharan African countries made significant efforts to develop a shared vision to counter cybercrime and the misuse of advanced technologies.

However, all their attempts to establish effective supranational instruments that would regulate the fight against cyberattacks at the Pan-African level and take into account the interests of the vast majority of African countries in this area have failed. This demonstrates the serious contradictions between African countries, which together hinder mutually beneficial cooperation even in the important area of cybersecurity.

However, until such cooperation emerges, it seems unlikely that African countries will even come close to solving this problem, which means that their information space will continue to be subject to large-scale cyber-attacks, posing a serious threat not only to the security of individuals, but also to national and pan-African security.

Received / Поступила в редакцию: 10.03.2022

Revised / Доработана после рецензирования: 03.04.2022

Accepted / Принята к публикации: 18.04.2022

References

- Antinori, A. (2019). Terrorism and deepfakes: From hybrid warfare to post-truth warfare in a hybrid world. In P. Griffiths & M. Nowshade (Eds.), *Proceedings of the European conference on the impact of artificial intelligence and robotics* (pp. 23—20). Reading, South Oxfordshire, England: Academic Conferences and publishing limited.
- Artificial intelligence for Africa: An opportunity for growth, development, and democratisation. (2018). *Access Partnership*. Retrieved from https://www.up.ac.za/media/shared/7/ZP_Files/ai-for-africa.zp165664.pdf
- Bazarkina, D. Y., & Pashentsev, E. N. (2019). Artificial intelligence and new threats to international psychological security. *Russia in Global Affairs*, 17(1), 147—170. <https://doi.org/10.31278/1810-6374-2019-17-1-147-170>
- Bazarkina, D. Y., Pashentsev, E. N., & Simons, G. (2020). *Terrorism and advanced technologies in psychological warfare: New risks, new opportunities to counter the terrorist threat*. New York: Nova Science Publishers.
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., et al. (2018). The malicious use of artificial intelligence: forecasting, prevention, and mitigation. *Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, OpenAI*, 1—100. Retrieved from <https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf>
- Butcher, N., Wilson-Strydom, M., & Baijnath, M. (2021). Artificial intelligence capacity in Sub-Saharan Africa. Compendium Report. *International Development Research Centre*. Retrieved from <https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/59999/27ea1089-760f-4136-b637-16367161edcc.pdf?sequence=1>
- Chesney, R., & Citron, D. (2018). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(1753), 1753—1820. <https://doi.org/10.15779/Z38RV0D15J>
- Chiluwa, I. E. (2019a). Deception in online terrorist propaganda: A study of ISIS and Boko Haram. In I. E. Chiluwa & S. A. Samoilenko (Eds.), *Handbook of research on deception, fake news, and misinformation online* (pp. 520—537). Hershey, PA: Information Science Reference. <https://doi.org/10.4018/978-1-5225-8535-0.ch028>
- Chiluwa, I. E. (2019b). Discourse analysis and conflict studies. In *SAGE Research Methods Cases*. London: SAGE Publications. <https://dx.doi.org/10.4135/9781526468208>
- Chiluwa, I. E. (2019c). Online activism in Mali: A study of digital discourses of the movement for the liberation of Azawad. In I. E. Chiluwa & G. Bourvier (Eds.), *Activism, campaigning and political discourse on Twitter* (pp. 207—234). New York: Nova Science Publishers.
- Chiluwa, I. E., Chimuanya, L., & Ajiboye, E. (2020). Communicating religious extremism in West Africa. In J. Tarusarira & E. Chitando (Eds.), *Themes in religion and human security in Africa* (pp. 166—179). London: Routledge. <https://doi.org/10.4324/9781003017080-12>
- Dack, S. (2019). Deep fakes, fake news, and what comes next. *The Henry M. Jackson School of International Studies, University of Washington*. Retrieved from <https://jsis.washington.edu/news/deep-fakes-fake-news-and-what-comes-next>
- Haula, K., & Agbozo, E. (2020). A systematic review on unmanned aerial vehicles in Sub-Saharan Africa: A socio-technical perspective. *Technology in Society*, 63, 1—7. <https://doi.org/10.1016/j.techsoc.2020.101357>

- Interpol. (2020). Online African organized crime from surface and dark web. *Interpol Analytical Report*. Retrieved from: <https://www.euneighbours.eu/sites/default/files/publications/2020-08/INTERPOL%20report.pdf>
- Ishengoma, F. R. (2013). Online social networks and terrorism 2.0 in developing countries. *International Journal of Computer Science and Network Solutions*, 1(4), 1—12. <https://doi.org/10.48550/arXiv.1410.0531>
- Jeangène Vilmer, J.-B., Escorcía, A., Guillaume, M., & Herrera, J. (2018). Les manipulations de l'information: un défi pour nos démocraties. *Rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées*, 1—214. Retrieved from https://www.diplomatie.gouv.fr/IMG/pdf/les_manipulations_de_l_information_2_cle04b2b6.pdf
- Kharouni, L. (2013). Africa: A new safe harbor for cybercriminals? *Trend Micro Incorporated Research Paper*, 1—31. Retrieved from <https://web.archive.org/web/20220403192613/https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf>
- Owoyemi, A., Owoyemi, J., Osiyemi, A., & Boyd, A. (2020). Artificial intelligence for healthcare in Africa. *Frontiers in Digital Health*, 2, 1—5. <https://doi.org/10.3389/fdgth.2020.00006>
- Pashentsev, E. (2019). Destabilization of unstable dynamic social equilibriums through high-tech strategic psychological warfare. In N. van der Waag-Cowling & L. Leenen (Eds.), *Proceedings of the 14th International Conference on Cyber Warfare and Security* (pp. 322—328). Reading, South Oxfordshire, England: Academic Conferences and publishing limited.
- Vattapparamban, E., Güvenç, İ, Yurekli, A., Akkaya, K., & Uluğaç S. (2016). Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 216—221). New York: Institute of Electrical and Electronics Engineers. <https://doi.org/10.1109/IWCMC.2016.7577060>

About the author: *Pantserev Konstantin Arsenievich* — PhD, Dr. of Sc. (Political Sciences), Professor, Department of Theory and History of International Relations, The Faculty of International Relations, St. Petersburg State University; ORCID: 0000-0002-2164-9525; e-mail: pantserev@yandex.ru



DOI: 10.22363/2313-0660-2022-22-2-303-319

Научная статья / Research article

Цифровой вызов для арабского мира: фактор интеграции или дифференциации?

Г.Н. Валиахметова  , Л.В. Цуканов 

Уральский федеральный университет имени Первого Президента России Б.Н. Ельцина,
Екатеринбург, Российская Федерация
vgulnara@mail.ru

Аннотация. По мере интеграции в глобальное цифровое пространство арабские страны разделяют его преимущества и риски, включаются в построение системы международной информационной безопасности. Учитывая значительное влияние арабского мира на формирование мировой политической повестки и глобальную систему безопасности, изучение специфики развития арабского цифрового кластера на современном этапе приобретает не только академическую, но и политическую актуальность. Статья посвящена исследованию текущего состояния, потенциала и пределов кооперации арабских стран в области цифровой защиты в рамках межарабского сотрудничества в многосторонних и двусторонних форматах, а также взаимодействия с мировыми лидерами технологической «гонки». Анализ основан на методологии Глобального индекса кибербезопасности, разработанной Международным союзом электросвязи ООН и включающей пять ключевых параметров оценки готовности современных государств к отражению киберугроз, таких как: нормативно-правовая система национальной киберзащиты, технические возможности, организационная структура, меры по развитию потенциала и международное сотрудничество. Оценивая «цифровой ландшафт» арабских государств, авторы отмечают, что политическая, финансово-экономическая и историко-культурная специфика арабских стран способствует формированию в регионе особой среды для противостояния киберугрозам и решения проблем кибербезопасности. С одной стороны, цифровой вызов побуждает арабские государства к преодолению некоторых разногласий, придавая определенный импульс интеграционным процессам. С другой стороны, «догоняющий» тип и скачкообразная динамика развития цифровой отрасли в регионе, а также присущая арабскому миру разнородность и противоречивость в совокупности с традиционно высокой степенью конфликтности в регионе и сильным влиянием внешних факторов создают гетерогенную и фрагментированную среду, препятствующую формированию коллективного ответа на вызовы цифровой эпохи.

Ключевые слова: арабские страны, Ближний Восток, киберугрозы, кибербезопасность, региональные международные отношения, интеграция

Для цитирования: Валиахметова Г. Н., Цуканов Л. В. Цифровой вызов для арабского мира: фактор интеграции или дифференциации? // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 303—319. <https://doi.org/10.22363/2313-0660-2022-22-2-303-319>



Digital Challenge for the Arab World: Integration or Differentiation Factor?

Gulnara N. Valiakhmetova ✉, Leonid V. Tsukanov 

Ural Federal University, Yekaterinburg, Russian Federation

✉vgulnara@mail.ru

Abstract. As Arab states integrate into the global digital space, they share its advantages and risks and are included in the construction of the international information security system. Considering the significant influence of the Arab world on the formation of the world political agenda and the global security system, the study of the specifics of the development of the Arab digital cluster at the present stage acquires not only academic but also political relevance. This article is devoted to the study of the current state, potential and limits of Arab countries cooperation in the field of digital security within the framework of inter-Arab cooperation in multilateral and bilateral formats, as well as interaction with the world leaders in the technological ‘race’. The analysis was based on the methodology of the Global Cybersecurity Index developed by the UN International Telecommunication Union. It includes five key parameters for assessing the readiness of modern states to repel cyberthreats: the regulatory and legal system of national cyber defense, technical capabilities, organizational structure, capacity development measures and international cooperation. Assessing the ‘digital landscape’ of the Arab states, the authors note that the political, financial, economic, historical, and cultural specifics of the Arab countries contribute to the formation of a special environment in the region for countering cyber threats and solving cyber security problems. On the one hand, the digital challenge is forcing the Arab states to overcome some differences, giving a certain impetus to integration processes. On the other hand, the ‘catch-up’ type, and spasmodic dynamics of the digital industry development in the region, as well as the heterogeneity and inconsistency inherent in the Arab world, combined with the traditionally high degree of conflict and the strong influence of external factors, create a heterogeneous and fragmented environment that prevents the formation of a collective response to challenges of the digital age.

Key words: Arab states, the Middle East, cyber threats, cyber security, regional international relations, integration

For citation: Valiakhmetova, G. N., & Tsukanov, L. V. (2022). Digital challenge for the Arab world: Integration or differentiation factor? *Vestnik RUDN. International Relations*, 22(2), 303—319. <https://doi.org/10.22363/2313-0660-2022-22-2-303-319>

Введение

Цифровизация как глобальный мегатренд порождает общий для всех стран комплекс угроз. Вместе с тем региональный контекст формирует специфику цифрового вызова, побуждая государства набирать собственные подходы и практики преодоления или снижения новых рисков. Арабский кейс представляет особый академический и практический интерес не только в связи с высоким влиянием арабского мира и шире — Большого Ближнего Востока¹ — на глобальную повестку. Взаимо-

действие общемировых и региональных трендов в этой части света носит сложный и противоречивый характер, причем развитие на региональном уровне может как обгонять, так и тормозить или даже противодействовать глобальным тенденциям, формируя порой противоположные им по направленности и характеру последствия (Барановский, Наумкин, 2018; Звягельская, Свистунова, Сурков, 2020b).

Научное осмысление особенностей развития Ближнего Востока в меняющемся глобальном контексте сопровождается разработкой новых теоретических подходов и изучением возможностей их применения к региональным реалиям. Отличительной чертой трудов российских востоковедов, ближневосточников и арабистов является сочетание политического или экономического анализа с методами

¹ В рамках данного исследования условный термин «арабский мир» обозначает геополитическое пространство, охватывающее 22 страны, входящие в состав Лиги арабских государств (ЛАГ), главной площадки межарабского сотрудничества. Арабский мир является системообразующим элементом ближневосточной подсистемы международных отношений и, в более расширительных трактовках, Большого Ближнего Востока (англоязычный аналог — регион MENA, Middle East

and North Africa), под которым в данной статье понимается геополитический регион в составе арабских стран, Турции, Ирана и Израиля.

исторического исследования, что позволяет строить прогнозные сценарии с учетом исторической специфики региона (Звягельская, Кузнецов, 2017; Мелкумян, 2020; Филоник, Исаев, 2020).

В рамках данного подхода В.Г. Барановский и В.В. Наумкин раскрывают особенности преломления глобальных мегатрендов на реалии Ближнего Востока, формирования регионального пространства и общей региональной идентичности, базирующейся на арабском компоненте. Поскольку становление государственности в арабских странах пришлось на колониальный период, неизменными атрибутами региона стали постоянный дефицит безопасности, эксклюзивизм (консолидация в противостоянии «чужим»), которыми в разное время считались Турция, Израиль, а в настоящее время Иран), высокая степень участия глобальных акторов в региональных делах и «эффект привыкания» к присутствию в регионе внешних интересов, а также перманентно растущая конфликтность на фоне ослабления субрегиональной интеграции (Барановский, Наумкин, 2018).

Анализ взаимодействия на Ближнем Востоке глобальных и региональных трендов через призму концепции «негативной неопределенности» приводит исследователей-международников к аналогичным выводам о дерегионализации и фрагментации имеющихся в арабском мире интеграционных площадок, о поддержании единства региона за счет высокого уровня конфликтности. Приметами современного ближневосточного политического ареала становятся также рост регионального соперничества и активности региональных держав, стремящихся использовать внешние интересы для реализации собственных амбиций; высокая степень недоверия и подозрительности, непрочность двусторонних отношений и расширение практики создания тактических альянсов (ситуативных союзов), в том числе с внешними акторами; ослабление интереса США и стран Запада к региону и, как следствие, их стремление к сокращению своего участия в региональной повестке; снижение роли «мягкой силы» и замещение ее инструментами «жесткой силы» в форме прокси-войн и прямых интервенций (Звягельская, Свистунова, Сурков, 2020b; Шумилин, 2019).

Понятие «неопределенность» также вошло в научный лексикон исследователей социально-экономического среза ближневосточных реалий. Разнообразие экономических моделей, наличие внушительного экономического, технологического и социального разрыва между арабскими странами, который усиливается снижающейся ролью большинства арабских экономик в мировом хозяйстве, создают условия для роста напряженности в регионе и оставляют мало места для интеграционных инициатив (Мельянцев, 2020; Филоник, Исаев, 2020).

Российские ученые обогащают собственными подходами концепции, разработанные в зарубежных научных сообществах. В рамках развития неомодернистского подхода, альтернативного модернизму и постмодернизму, В.А. Кузнецов исследует проблему преодоления социально-политических фрагментаций арабских сообществ (Кузнецов, 2019; 2020). Ученые ИМЭМО РАН систематизируют обширный пласт концепций политической идентичности, выявляя факторы выбора внешнеполитических приоритетов для ближневосточных государств (Звягельская и др., 2020a). Феномен перманентно возрастающей конфликтности и меняющейся роли внешних акторов в обеспечении безопасности на Ближнем Востоке исследуется в трудах В.В. Наумкина на основе концептов территориального и демографического «упорядочивания» (Наумкин, 2019) и теории глубоко разделенных обществ (Наумкин, 2015).

Эмпирический материал Ближнего Востока позволяет коллективу исследователей из МГИМО МИД России опровергнуть популярную за рубежом теорию волн демократизации, на основе которой западные авторы отстаивают тезис о положительном влиянии информационных технологий на демократический выбор современных государств. Российские ученые убедительно доказывают, что экстраполяция глобального тренда цифровизации на арабские страны с их поздней субъектностью в системе международных отношений, незавершенностью нацистроительства, гибридной политическими системами, сочетающими традиционные и современные элементы, а также многочисленными дисбалансами

институционального развития способны породить откат государств к авторитаризму и даже архаизации (Лебедева и др., 2016). Другим примером критического подхода к аналитическому потенциалу западных концепций может служить исследование Е.С. Зиновьевой (Зиновьева, 2018), научная новизна которого обусловлена применением методологического инструментария теории социального конструктивизма для изучения взаимовлияния научно-технологической сферы и мирополитических процессов.

Проблемы построения в арабском мире коллективной системы кибербезопасности относительно недавно появились в политической и научной повестке и пока мало изучены как в России, так и за рубежом. В российском академическом поле цифровая проблематика региона представлена преимущественно исследованиями феномена кибертерроризма и роли информационно-коммуникационных технологий (ИКТ) в мобилизации протестного ресурса на примере событий «арабской весны». Страновые кейсы охватывают, как правило, неарабские государства Ближнего Востока — Иран, Израиль и Турцию. Схожая картина наблюдается в зарубежных публикациях, однако представители западных и ближневосточных научных сообществ активнее обращаются к арабской тематике, расширяя эмпирическую и аналитическую базу исследований по проблемам общерегиональной кибербезопасности. В данном контексте следует отметить труды, посвященные практикам цифровой защиты отдельных арабских стран (Alaleeli & Alnajjar, 2020; El-Houssami & Rizk, 2020; Shat et al., 2013), роли внешних акторов (Liu, 2021; Mogielnicki, 2021) и Израиля² в обеспечении кибербезопасности ведущих экономик региона, а также различным аспектам цифрового вызова, требующего от арабских

стран коллективного ответа (Alrawabdeh, 2009; Röpper et al., 2021).

В целом, несмотря на исключительное разнообразие подходов и тематик исследований по специфике трендов развития арабского мира, в том числе в контексте информационных угроз, проблемы переформатирования региона в единое пространство кибербезопасности пока фрагментарно представлены в научных публикациях. Данная статья позволяет в определенной степени восполнить указанный пробел в рамках поиска ответа на вопрос, сможет ли цифровой вызов стать тем фактором, который позволит арабскому миру преодолеть его традиционную противоречивость и объединиться для разработки коллективного ответа.

Общетеоретической основой исследования стали фундаментальные труды крупнейшего исследователя информационной эпохи М. Кастельса (Castells, 2002; 2010), что позволило рассматривать арабский мир не только как самостоятельный кластер, но и как часть глобального цифрового общества. Оценка текущего состояния готовности арабских стран к отражению цифровых угроз произведена преимущественно на основе методологии Глобального индекса кибербезопасности (Global Cybersecurity Index, GCI) — исследовательского мегапроекта Международного союза электросвязи (МСЭ) ООН³. При составлении рейтинга эксперты МСЭ принимали во внимание пять критериев: нормативно-правовую систему национальной киберзащиты, технические возможности, организационную структуру, меры по развитию потенциала, международное сотрудничество. В рамках данного исследования указанные параметры будут рассматриваться через призму проблематики межарабского сотрудничества и взаимодействия арабского мира с внешними акторами. В работе использованы методы структурного, системного и статистического анализа, ивент-анализа и сценарного прогнозирования.

² См.: El-Masry J. The Abraham Accords and Their Cyber Implications: How Iran is Unifying the Region's Cyberspace // Middle East Institute. June 9, 2021. URL: <https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace> (accessed: 30.10.2021); Khorrami N. One Year On — Israel's Cybersecurity Cooperation with the GCC States // Middle East Institute. September, 2021. URL: <https://mei.nus.edu.sg/wp-content/uploads/2021/09/Insight-266-Nima-Khorrami.pdf> (accessed: 30.10.2021).

³ Global Cybersecurity Index (далее — GCI) 2014—2020. Geneva: International Telecommunication Union (ITU), 2015—2021. URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx> (accessed: 30.10.2021).

Специфика арабского пространства цифровых угроз

Процессы цифровизации стартовали в арабском мире почти на десятилетие позже, чем в странах Глобального Севера. В 2000-х гг. регион продемонстрировал взрывной рост численности интернет-пользователей, в 2015 г. превысил средние общемировые показатели и в 2019 г. достиг 62,96 %⁴. Хотя по степени проникновения Интернета арабский компонент Глобального Юга еще значительно отстает от государств Организации экономического сотрудничества и развития (ОЭСР) (85,08 %)⁵, по численности абонентов мобильной сотовой связи на 100 человек этот разрыв уже незначителен (103,2 и 120,2 чел. соответственно)⁶.

В авангарде движения к цифровому обществу находятся монархии Персидского залива, где уровень проникновения Интернета за последнее десятилетие удвоился и сейчас составляет от 95 % и выше, опережая по данному параметру лидеров Глобального Севера, а Объединенные Арабские Эмираты (ОАЭ) стали первым и пока единственным государством мира с численностью интернет-пользователей в 100 %⁷. На противоположном полюсе арабского мира расположены наименее развитые и политически нестабильные страны с уровнем проникновения Интернета от 30 % и ниже; в «средней» группе государств указанный показатель варьируется в диапазоне 57,2—72 %⁸. Рост интернет-активности увеличивает риск кибератак, формируя в этом разнородном и противоречивом регионе различные виды угроз.

Благодаря успешной модернизации, диверсификации и цифровизации своих

экономик в рамках масштабных долгосрочных программ «Видение» наиболее быстро наращивают свое присутствие в киберпространстве аравийские монархии. Именно они становятся главными мишенями для финансово ориентированной киберпреступности, ущерб от которой в этих странах исчисляется миллиардами долларов⁹. Вместе с тем, в отличие от других регионов, в арабском мире кибератаки ориентированы преимущественно на доступ к коммерческим, технологическим и государственным секретам (63,6 %), нежели на похищение финансовых (6,2 %) и персональных данных (29,6 %)¹⁰.

По количеству кибератак региональный рейтинг традиционно возглавляли монархии Залива, но в последние годы они значительно усилили свою защиту: в 2021 г. Королевство Саудовская Аравия (КСА) и ОАЭ опустились соответственно на 3-е и 4-е места в арабском индексе (30-я и 36-я строки в мировом)¹¹. Тем не менее они наряду с США остаются в тройке

⁹ См.: El-Masry J. The Abraham Accords and Their Cyber Implications: How Iran is Unifying the Region's Cyberspace // Middle East Institute. June 9, 2021. URL: <https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace> (accessed: 30.10.2021); The New Battlefield: Cyber Security across the GCC // Gulf International Forum. October 29, 2018. URL: <https://gulffif.org/the-new-battlefront-cyber-security-across-the-gcc/> (accessed: 30.10.2021).

¹⁰ Data Breach Report 2018. A Study of Data Leaks in the Middle East // InfoWatch Analytics Center, 2018. P. 4. URL: https://infowatch.com/sites/default/files/report/analytics/a_study_of_data_leaks_in_the_middle_east_in_2017-2018.pdf (accessed: 30.10.2021). Этой спецификой объясняется внушительный рост кибератак в зоне Залива в периоды подготовки и проведения таких крупных мировых событий, как Dubai Expo 2020 и Qatar World Cup 2022. Эксперты Международного форума стран Персидского залива, отмечают, что «74 % руководителей предприятий региона рассматривают риск нарушений конфиденциальности данных как наиболее актуальную угрозу доверию заинтересованных сторон к бизнесу, что намного выше, чем в среднем по миру (55 %)». Цит. по: The New Battlefield: Cyber Security across the GCC // Gulf International Forum. October 29, 2018. URL: <https://gulffif.org/the-new-battlefront-cyber-security-across-the-gcc/> (accessed: 30.10.2021).

¹¹ По состоянию на 31 декабря 2021 г. См.: Kaspersky Cyberthreat Real-Time Map. URL: <https://cybermap.kaspersky.com/> (accessed: 31.12.2021).

⁴ Individuals Using the Internet (% of population) // Data Bank World Development Indicators. URL: <https://data.worldbank.org/indicator/IT.NET.USER.ZS> (accessed: 30.11.2021).

⁵ Ibid.

⁶ Mobile Cellular Subscription (per 100 people) // Data Bank World Development Indicators. URL: <https://databank.worldbank.org/reports.aspx?source=2&series=IT.CEL.SETS.P2&country=VNM> (accessed: 30.11.2021).

⁷ Individuals Using the Internet (% of population) // Data Bank World Development Indicators. URL: <https://data.worldbank.org/indicator/IT.NET.USER.ZS> (accessed: 30.11.2021).

⁸ Ibid.

мировых лидеров с самыми дорогостоящими утечками данных¹².

Критически важным активом аравийских монархий является нефтегазовый сектор, предприятия которого, как правило, сосредоточены в узких географических областях, что значительно увеличивает урон от кибератак. В последнее десятилетие саудовский нефтегазовый гигант Saudi Aramco и катарский RasGas неоднократно становились жертвами крупных нападений с использованием сложных вирусных программ (2012, 2016, 2017 г.) и беспилотников (2019 г.). Подобные атаки имеют не только глобальные экономические последствия — от повышения цен на нефть до каскадного воздействия на различные отрасли мировой экономики (Rörper et al., pp. 96—97). Речь идет о применении так называемых цифровых вооружений, за разработкой которых стоят государства, в связи с чем такие атаки интерпретируются как акт внешней агрессии, создавая потенциал для ответного киберудара (Савельев, Карасев, 2018).

Высокая степень киберугроз со стороны государственных субъектов региональной и мировой политики, а также относительно низкий уровень готовности арабских стран к их отражению являются еще одной особенностью региона¹³. Практика применения прорывных цифровых технологий в качестве силовой компоненты в межгосударственных конфликтах получила широкое распространение на Ближнем Востоке после кибератаки на ядерный исследовательский центр Ирана в 2010 г. с использованием вируса нового поколения Stuxnet, который был признан первым образцом кибероружия в силу его колоссального разрушительного потенциала. Масштабные испытания кибероружия, проводившиеся на Ближнем Востоке в 2010—2012 гг. предположительно

¹² Устранение последствий каждого из подобных нарушений по стоимости составляет в среднем более 5 млн долл. США, может занять несколько месяцев и нанести серьезный финансово-экономический и репутационный ущерб. См.: Internet Infrastructure Security Guidelines for the Arab States // Internet Society. March 2020. P. 6. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

¹³ Ibid.

США и Израилем¹⁴, втянули в гонку цифровых вооружений сначала Иран, а затем и другие страны региона.

В 2015 г. появились данные о причастности правительств Бахрейна, Египта, КСА, Ливана, Марокко, ОАЭ, Омана и Судана к покупке за рубежом шпионского программного обеспечения (ПО) и других вредоносных цифровых инструментов¹⁵. Тайное сотрудничество с Израилем, одним из лидеров глобального рынка кибервооружений, обеспечило ряд монархий Залива эффективными инструментами противодействия Ирану, борьбы с терроризмом и контроля за внутренней оппозицией¹⁶. Межгосударственное противостояние в киберпространстве Ближнего Востока пролегал прежде всего по линиям КСА — Иран, Израиль — Иран, США — Иран, а также реализуется в контексте региональных кризисов (сирийского, йеменского, катарского и т. д.). При этом цифровые вооружения, используемые, например, в саудовско-иранском прокси-конфликте в Йемене, применяются на всем Ближнем Востоке и за его пределами¹⁷. Использование арабскими странами ИКТ в качестве инструмента внешней и внутренней

¹⁴ Паю К., Эмм Д. Kaspersky Security Bulletin 2013: Развитие угроз в 2013 году // Securelist. 11.12.2013. URL: <https://securelist.ru/analysis/ksb/19140/kaspersky-security-bulletin-2013-razvitie-ugroz-v-2013-godu/> (дата обращения: 21.10.2021). Сегодня средства ведения цифровых войн (кибервойн) варьируются от относительно несложных хакерских программ до ИКТ, приравненных к стратегическим наступательным вооружениям, причем серьезный материальный или политический ущерб государству может быть нанесен и технически слабо подготовленными, но массовыми группами, использующими широко доступные вирусные программы (например, хактивистами в рамках протестных акций). См., например: (Каберник, 2013).

¹⁵ Неизвестные взломали сеть поставщика шпионского ПО для правительственных спецслужб // SecureLab. 06.07.2015. URL: <http://www.securitylab.ru/news/473587.php> (дата обращения: 21.11.2021).

¹⁶ Khorrami N. One Year On — Israel's Cybersecurity Cooperation with the GCC States // Insights. 2021. No. 266. P. 1—2. URL: <https://mei.nus.edu.sg/wp-content/uploads/2021/09/Insight-266-Nima-Khorrami.pdf> (accessed: 30.10.2021).

¹⁷ От Shamoon к StoneDrill. Wiper-подобные программы атакуют компании в Саудовской Аравии и не только // SecureList. 06.03.2018. URL: <https://securelist.ru/from-shamoon-to-stonedrill/30350/> (дата обращения: 21.11.2021).

политики значительно ухудшает региональную среду, увеличивая ее и без того высокий конфликтный потенциал.

Помимо государств носителями угроз в арабском цифровом пространстве являются внесистемные игроки региональной политики в лице кибергрупп, предположительно спонсируемых на государственном уровне, а также хактивисты и хакеры-одиночки, активность которых тоже зачастую выходит далеко за рамки Ближнего Востока. Кроме того, глобализация киберугроз, исходящих из региона, обусловлена деятельностью многочисленных радикально-экстремистских и террористических группировок, которые ведут в Глобальной сети киберджихад против «неверных»¹⁸.

Таким образом, из триады киберугроз, в контексте которой ООН определяет понятие «международная информационная безопасность», для арабского мира первостепенное значение имеет угроза использования ИКТ в военно-политических целях, в качестве инструмента межгосударственного противостояния и вмешательства во внутренние дела суверенных государств. Противодействие данному виду угроз напрямую зависит от стабилизации военно-политической обстановки и урегулирования многочисленных конфликтов на Ближнем Востоке, что, в свою очередь, требует объединения усилий региональных акторов и поддержки со стороны международного сообщества. Другие виды угроз — киберпреступность и кибертерроризм — также формируют общий для арабских стран вызов, побуждая развивать кибербезопасность не только на национальном, но и региональном уровне.

Кибербезопасность в арабском мире: тенденции и проблемы развития

В последние годы ряд арабских государств довольно внушительно усилили свои позиции в Глобальном индексе кибербезопасности МСЭ. Наиболее впечатляющие результаты — у КСА и ОАЭ, которые в 2020 г.

¹⁸ EU Terrorism Situation and Trend Report (TE-SAT) 2019. Hague : European Police Office, 2019. URL: <https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat> (accessed: 19.10.2021). См. также: (Bunt, 2003).

вошли в пятерку мировых лидеров; «спринтерский» подход демонстрируют также Катар, Кувейт и Иордания¹⁹. Для Омана и Египта²⁰, Туниса, Марокко и Бахрейна, которые первыми из арабских стран приступили к созданию систем национальной кибербезопасности, характерен поступательный тип развития. В указанной региональной десятке лидеров индекс МСЭ варьируется от 99,5 (КСА) до 70,9 (Иордания). Остальные арабские государства имеют низкий уровень киберзащиты, занимая 104—182-ю строки глобального рейтинга с индексом ниже 35²¹. В целом анализ данных МСЭ свидетельствует о «догоняющем» типе развития национального сектора кибербезопасности и наличии значительного цифрового разрыва между странами арабского мира.

В сфере нормативно-правового обеспечения цифровой защиты большинство арабских стран уже сделали серьезные шаги: 17 государств имеют законы о несанкционированном доступе к информации, 14 — о защите данных, 12 — о мерах по уведомлению о нарушениях, 11 — об антиобщественном поведении в Интернете²². По данному показателю

¹⁹ КСА и ОАЭ поднялись соответственно с 46-й и 47-й позиций глобального рейтинга 2017 г. на 2-ю и 5-ю строки в 2020 г. Кувейт переместился с 138-го места в 2017 г. на 64-ю строку в 2020 г. и с 17-го на 9-е место в арабском рейтинге. См.: GCI 2017. P. 59—64. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (accessed: 30.10.2021); GCI 2020. P. 25—27, 29. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

²⁰ До 2020 г. Оман и Египет с большим отрывом лидировали в региональном рейтинге кибербезопасности, а Оман входил в тройку мировых лидеров в 2014 г. и занимал 4-е место в мире в 2017 г. В 2020 г. обе страны спустились в Индексе МСЭ соответственно на 21-е и 23-е места (3-я и 4-я позиции в арабском регионе), продолжая, тем не менее, опережать ряд европейских государств. См.: GCI 2015. P. 1. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf (accessed: 30.10.2021); GCI 2017. P. 59. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (accessed: 30.10.2021); GCI 2020. P. 25—27, 29. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

²¹ GCI 2020. P. 25—27. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021). Максимальное значение индекса МСЭ — 100.

²² Ibid. P. 3—6.

арабский мир демонстрирует тренды, схожие с другими регионами: наличие правовых норм по предупреждению и противодействию преступной деятельности в киберпространстве, как правило, характерно для стран с высоким и средним уровнем проникновения Интернета, устойчивой экономикой и нацеленностью правительств на цифровизацию²³. Вместе с тем в арабском мире, где ислам регулирует различные сферы жизни, законотворческий процесс в той или иной мере требует согласования с нормами шариата²⁴, прежде всего нормами мусульманского права (фикха) (Сюкияйнен, 2016; 2019). В числе других факторов, тормозящих адаптацию национальных законодательств арабских стран к реалиям цифровой эпохи, следует отметить определенную инертность нормативно-правовой сферы, реактивный подход к заполнению образующихся в законодательстве лагун, купирование отдельных аспектов проблемы вместо комплексного решения, излишнюю бюрократизацию законотворческого процесса и т. д. Преодоление указанных барьеров откроет путь к гармонизации арабских законодательств и формированию региональной системы кибербезопасности²⁵.

Наличие групп реагирования на компьютерные инциденты (Computer Incident Response Teams, CSIRT) или групп реагирования на компьютерные чрезвычайные ситуации (Computer Emergency Response Team, CERT) является ключевым показателем для оценки МСЭ технических мер развития кибербезопасности.

²³ GCI 2020. P. 4—5. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

²⁴ Так, в КСА отсутствует уголовный кодекс и ряд других атрибутов романо-германской правовой системы. Поскольку законодательство страны базируется на исламском праве, в правоприменительной практике преобладают нормы шариата, в том числе в области регулирования интернет-пространства. См.: Королевство Саудовская Аравия // Научно-технический центр ФГУП «ГРЧЦ». 29.03.2021. URL: <https://rdc.grfc.ru/2021/03/saudi-arabia/> (дата обращения: 21.11.2021). О специфике восприятия цифровизации в системе исламских ценностей см., например: (Faizi & Abubakar, 2021).

²⁵ Development and Harmonization of Cyber Legislation in the Arab Region. New York : Economic and Social Commission for Western Asia (ESCWA), 2013. URL: https://unctad.org/system/files/non-official-document/СИЕМ5_ESCWA2_en.pdf (accessed: 10.10.2021).

Модель CSIRT базируется на принципах открытости и сотрудничества и предполагает, что технико-технологическая защита может быть обеспечена не возведением «высоких стен» вокруг интернет-инфраструктуры, но созданием атмосферы доверия и условий для широкого обмена информацией и опытом²⁶.

Национальные CSIRT/CERT действуют в 17 арабских государствах, причем исключительно в статусе правительственных учреждений²⁷. В ряде стран их деятельность не ограничивается традиционной защитой цифровой инфраструктуры или оказанием прямой технической поддержки органам государственной власти, но также включает проведение информационно-просветительских кампаний и киберучений, аккредитацию экспертов по кибербезопасности и иные мероприятия по увеличению национального киберпотенциала, развитию и углублению отношений с различными субъектами кибербезопасности. В 10 арабских странах, кроме того, созданы отраслевые CSIRT, преимущественно в телекоммуникационном или энергетическом секторах²⁸.

По мнению экспертов, группы реагирования уже сыграли ключевую роль в защите интернет-структур арабских государств, однако их эффективность ограничивается нехваткой финансов, оборудования, специалистов и навыков, причем с такими проблемами сталкиваются не только слаборазвитые страны, но и передовые²⁹. Кроме того, в отличие от

²⁶ Internet Infrastructure Security. Guidelines for the Arab States // Internet Society. 2020. P. 1. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

²⁷ GCI 2020. P. 7. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

²⁸ См.: GCI 2020. P. 8. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021); Internet Infrastructure Security. Guidelines for the Arab States // Internet Society. 2020. P. 7, 12. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

²⁹ Так, CERT Бахрейна формировалась при спонсорском участии Вашингтона, заинтересованного в усилении безопасности крупнейшей на Ближнем Востоке военно-морской базы США, размещенной в этом шейхстве. См.: The New Battlefield: Cyber Security across the GCC // Gulf International Forum. October 29,

других регионов, арабские национальные CSIRT меньше сотрудничают с частным сектором и другими заинтересованными сторонами³⁰. Слабость горизонтальных связей CSIRT пока не позволяет ни одному арабскому государству достичь максимального показателя МСЭ по техническим мерам³¹.

Тем не менее в арабском мире наблюдается растущая тенденция к развитию государственно-частных партнерств на национальном уровне, особенно с появлением отраслевых CSIRT. Ряд стран нарабатывают методы и практики выявления и устранения правовых и иных барьеров для взаимодействия различных субъектов кибербезопасности — государственных учреждений, бизнес-структур, исследовательских сообществ, рядовых интернет-пользователей, а также внесистемных акторов в лице, например, «белых хакеров»³².

Препятствиями для создания устойчивой региональной цифровой инфраструктуры являются традиционная для арабского мира атмосфера недоверия и управленческая модель «нисходящего контроля» со стороны государства. При таком подходе различные госучреждения и подконтрольные правительствам CSIRT, действуя исходя из национальных приоритетов (в том числе в интересах национальных разведслужб), сталкиваются с

недоверием со стороны зарубежных коллег³³. Иными словами, в регионе имеется запрос на доверие и стратегическую гибкость.

Значительные шаги в этом направлении уже сделаны. В 2012 г. в Маскате был создан Региональный центр МСЭ по кибербезопасности для арабского региона³⁴ под оперативным управлением CERT Омана, который также отвечает за координацию CERT монархий Залива³⁵. Взаимодействие также осуществляется на полях Регионального саммита по кибербезопасности для арабских государств³⁶ и Организации исламского сотрудничества (ОИС)³⁷. Арабские страны, кроме того, участвуют в глобальных инициативах с целью углубления знаний в области кибербезопасности и выстраивания отношений на межгосударственном и межотраслевом уровнях. Так, 7 арабских государств (Катар, КСА, Египет, Марокко, ОАЭ, Оман, Тунис) сотрудничают в формате глобального Форума групп реагирования на инциденты и обеспечения безопасности. У КСА и ОАЭ — самое большое из арабских стран-участниц представительство — соответственно 9 и 5 правительственных и отраслевых групп³⁸.

Третий оценочный критерий МСЭ — организационные меры — включает механизмы управления и координации сферы кибербезопасности на уровне исполнительной власти, частного сектора и гражданского общества. Главным индикатором их эффективности является наличие и характеристики национальной стратегии кибербезопасности (НСК). Ее оценка осуществляется по ряду параметров:

³³ Ibid. P. 14.

³⁴ ITU Arab Regional Cybersecurity Centre (ITU-ARCC). URL: <https://arcc.om/?GetLang=en> (accessed: 10.12.2021).

³⁵ About OCERT // Oman National CERT. URL: <https://cert.gov.om/about.aspx> (accessed: 10.12.2021).

³⁶ 9-я по счету встреча прошла в КСА в ноябре 2021 г. вместе с ежегодной (13-й) конференцией групп CERT стран — участниц ОИС. См.: CERTs in an Evolving Cybersecurity Landscape. URL: <https://www.oic-cert.org/event2021/> (accessed: 10.12.2021).

³⁷ Online Tutoring — What It Is All about and How Much It Costs // OIC Tech Platform. September 2, 2018. URL: <http://www.oic-cert.net/> (accessed: 10.12.2021).

³⁸ FIRST Members around the World // FIRST. URL: <https://www.first.org/members/map> (accessed: 10.12.2021).

2018. URL: <https://gulrif.org/the-new-battlefront-cybersecurity-across-the-gcc/> (accessed: 30.10.2021). Другим примером служит КСА, где в рамках приоритета киберзащиты критической инфраструктуры власти взяли курс на постоянные централизованные закупки за рубежом (преимущественно в США) ПО и иных готовых решений. См.: Hathaway M., Spidaleri F., Alsowailm F. Kingdom of Saudi Arabia Cyber Readiness at a Glance // Potomac Institute for Policy Studies. September 2017. URL: <https://www.belfercenter.org/sites/default/files/files/publication/cr-2.0-ksa.pdf> (accessed: 17.10.2021).

³⁰ Internet Infrastructure Security. Guidelines for the Arab States // Internet Society. 2020. P. 7, 13—14. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

³¹ GCI 2020. P. 71—82. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

³² Internet Infrastructure Security. Guidelines for the Arab States // Internet Society. 2020. P. 14—16. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

— нацеленность на защиту критической инфраструктуры (имеется у 13 арабских стран);

— регулярные обновления в контексте новых угроз и приоритетов (6 государств);

— проведение национальных аудитов;

— наличие метрик для оценки рисков на национальном уровне (9 стран) и т. д.³⁹

Зависимость развития национальной цифровой отрасли и кибербезопасности от внешней помощи, прежде всего в лице ООН и стран Глобального Севера, формирует в арабском мире схожие с ними методологические подходы к понятию «кибербезопасность», которое синонимично термину «информационная безопасность» и охватывает широкий круг проблем, связанных с технико-технологической защитой информационных систем и сетей⁴⁰.

Сегодня максимальный показатель МСЭ по организационным мерам достигнут только тремя арабскими государствами — КСА, Оманом и Египтом; высокий индекс также у ОАЭ и Катара⁴¹, остальным странам еще предстоит устранять серьезные пробелы в системе управления киберзащитой. Пробуксовка в

разработке НСК, институционализации и централизации кибербезопасности на одной платформе обусловлена в арабских странах реактивным, а не проактивным подходом к парированию угроз, «нисходящей» моделью управления, порождающей множество правительственных институтов с зачастую дублирующим функционалом и низкий уровень межведомственного взаимодействия, а также ограниченностью финансовых и кадровых ресурсов, слабостью горизонтальных связей между различными субъектами кибербезопасности⁴² (Röpper et al., 2021, p. 97). Кроме того, инвестиции в кибербезопасность реализуются преимущественно через программы модернизации военного потенциала и защиты наиболее значимых отраслей (энергетической, финансовой и ИКТ)⁴³, что обусловлено экономической и военно-политической спецификой региона.

По мнению исследователей, ключевую роль в устранении фрагментации саудовского пространства кибербезопасности сыграли США, заложив данную задачу в качестве одного из основных компонентов соглашения 2017 г. по модернизации вооруженных сил КСА стоимостью 110 млрд долл. США⁴⁴. Повышение киберготовности для обеспечения безопасности, как собственной, так и внешних партнеров, характерно для тех арабских стран, которые имеют военно-политическую и/или экономическую значимость для внерегиональных акторов. Этим объясняется наращивание национального киберпотенциала при активном участии внешних сил не только в передовых государствах региона, но и в наименее

³⁹ GCI 2020. P. 10—13. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021). Последний из указанных параметров реализуется также на региональном уровне на онлайн-платформе Регионального центра МСЭ в Омане, где все арабские страны имеют возможность произвести оценку своих киберрисков в режиме текущего времени. См.: About OCERT Services // Oman National CERT. URL: <https://cert.gov.om/services.aspx> (accessed: 10.12.2021).

⁴⁰ См., например: National Cybersecurity Strategy // UAE Telecommunication and Digital Government Regulatory Authority. URL: <https://tdra.gov.ae/en/national-cybersecurity-strategy> (accessed: 15.12.2021); Egypt National Cybersecurity Strategy (2017—2021) // Ministry of Communications and Information Technology. URL: https://www.mcit.gov.eg/Upcont/Documents/Publications_12122018000_EN_National_Cybersecurity_Strategy_2017_2021.pdf (accessed: 15.12.2021); Developing National Information Security Strategy for the Kingdom of Saudi Arabia // Kingdom of Saudi Arabia Ministry of Communications and Informational Technology. March 10, 2017. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SaudiArabia_NISS_Draft_7_EN.pdf (accessed: 15.12.2021).

⁴¹ GCI 2020. P. 71—82. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

⁴² Internet Infrastructure Security. Guidelines for the Arab States // Internet Society. 2020. P. 14—16. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

⁴³ Cybersecurity Spending for Critical Infrastructure to Surpass US\$105 Billion in 2021 // ABI Research. February 10, 2021. URL: <https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/> (accessed: 10.12.2021).

⁴⁴ См.: U.S. Security Cooperation with Saudi Arabia. Fact Sheet // U.S. State Department. January 20, 2021. URL: <https://www.state.gov/u-s-security-cooperation-with-saudi-arabia/> (accessed: 10.12.2021); The New Battlefield: Cyber Security across the GCC // Gulf International Forum. 2018. URL: <https://gulif.org/the-new-battlefront-cyber-security-across-the-gcc/> (accessed: 30.10.2021).

развитых, например в Сомали и Джибути⁴⁵, где расположены иностранные военные базы.

Государства, не представляющие интереса для внешних акторов в силу своей экономической отсталости или политической нестабильности, не могут рассчитывать на финансовую, технологическую и кадровую помощь извне. Так, снижение роли палестинского фактора в региональной повестке (Шумилин, 2019, с. 116; Наумкин, 2019, с. 75—78) привело к существенному сокращению внешней помощи Палестине в формировании национального сектора ИКТ и киберзащиты и, как следствие, падению рейтинга страны в Глобальном индексе МСЭ с 102 позиции в 2017 г. на 122 строку в 2020 г.⁴⁶ Иными словами, все более проявляющийся избирательный и прагматичный подход внешних спонсоров к поддержке программ цифровизации и кибербезопасности арабских стран будет оказывать возрастающее влияние на увеличение цифрового разрыва в арабском мире.

Четвертый показатель готовности государств к отражению киберугроз — меры по развитию потенциала — включает подготовку собственных кадров, наличие профильных образовательных программ и исследовательских институтов, поддержку малого и среднего бизнеса, развитие государственно-частного партнерства. По данному параметру максимальный индекс МСЭ имеют только 4 государства — Катар, КСА, ОАЭ и Оман, высокий

⁴⁵ US, France, Djibouti Enhance Cyber Defense Interoperability // Dvids. February 23, 2021. URL: <https://www.dvidshub.net/news/389582/us-france-djibouti-enhance-cyber-defense-interoperability> (accessed: 12.12.2021).

⁴⁶ См.: GCI 2017. P. 59—64. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (accessed: 30.10.2021); GCI 2020. P. 25—27. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021). О программах внешней помощи Палестине в сфере развития ИКТ и кибербезопасности подробнее см.: Modernising the Public Administration. The Case of E-Government in the Palestinian Authority. OECD, 2011; Telecommunication Sector Note in the Palestinian Territories: Missed Opportunity for Economic Development. Note for the Palestinian Ministry of Telecommunications and Information Technology. World Bank Group, 2016. 63 p.; Shahwan M.A.M. Suggesting the Best Information Security Management System for Palestinian E-Government. Tallinn, 2015. 74 p. См. также: (Shat et al., 2013).

показатель также у Египта, для остальных арабских стран — это сфера потенциального роста⁴⁷.

Хотя арабские правительства и признают значимость данной группы мер, они реализуются преимущественно с подачи и при поддержке западных партнеров⁴⁸. Кроме того, наблюдается серьезный дисбаланс в географии соглашений в области государственно-частного партнерства с участием двух и более арабских компаний: такое взаимодействие осуществляется главным образом между монархиями Залива, в то время как в остальной части арабского мира оно отсутствует либо ограничивается единичными эпизодами⁴⁹.

Серьезным вызовом для арабского мира становится также проблема «утечки мозгов», которая не нова для региона⁵⁰, однако именно с запуском реформ в области цифровизации она приобрела особую остроту. Несмотря на очевидные успехи⁵¹ в подготовке собственных кадров (Alaleeli & Alnajjar, 2020), отток профессионалов в страны Запада продолжается, причем для квалифицированных кадров из арабских стран даже ведущие экономики региона в лице государств Залива по своей

⁴⁷ GCI 2021. P. 71—82. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

⁴⁸ Christidis O. Technology and Youth Drive the Future of Work in MENA // Middle East Institute. October 22, 2021. URL: <https://www.mei.edu/publications/technology-and-youth-drive-future-work-mena> (accessed: 22.10.2021). См. также: (Pöpper et al., 2021, pp. 98—100).

⁴⁹ Закономерность выведена на основе анализа данных, содержащихся в открытых базах контрагентов арабских стран Ближнего Востока, а также реестра совместных с арабскими партнерами компаний, зарегистрированных в США. См., например: Public Register // Qatar Financial Centre. URL: <https://eservices.qfc.qa/qfcpublicregister/publicregister.aspx> (accessed: 12.12.2021).

⁵⁰ Stop the Brain Drain from the Arab World // Gulf News. December 29, 2003. URL: <https://gulfnews.com/uae/stop-the-brain-drain-from-the-arab-world-1.374254> (accessed: 14.12.2021).

⁵¹ См., например: Shaneen S. By 2030, Every 100 Saudi Residents Will Have “One Programmer” // Leaders. August 27, 2021. URL: <https://www.leaders-mena.com/by-2030-every-100-saudi-residents-will-have-one-programmer/> (accessed: 15.12.2021); Christidis O. Technology and Youth Drive the Future of Work in MENA // Middle East Institute. October 22, 2021. URL: <https://www.mei.edu/publications/technology-and-youth-drive-future-work-mena> (accessed: 22.10.2021).

привлекательности значительно уступают таким направлениям миграции, как США, ЕС и Канада⁵². С учетом оттока населения из турбулентных зон региона и существенного социально-экономического разрыва между арабскими странами, в том числе в индексе человеческого развития (Мельянцев, 2020), движение человеческого капитала будет усиливать технологическое неравенство в арабском мире и препятствовать его интеграции.

Международное сотрудничество арабских стран в области кибербезопасности

Международное сотрудничество является краеугольным камнем в системе обеспечения национальной и региональной кибербезопасности, однако именно по данному параметру позиции арабских стран наиболее уязвимы и свидетельствуют о наличии значительного «цифрового разрыва»⁵³. Как и в других регионах, в такой деликатной сфере, как кибербезопасность, арабские страны предпочитают входить в многосторонние соглашения (12 стран) и иные международные форматы участия (14 стран), нежели в двусторонние формы межгосударственного взаимодействия (11 стран)⁵⁴.

⁵² Migration in the Middle East and North Africa // Konrad Adenauer Stiftung. March 1, 2021. URL: <https://www.kas.de/documents/282499/282548/Migration+in+the+Middle+East+and+North+Africa+Report+KAS+PolDiMed+Survey.pdf/aec38c1f-bcf4-a58d-fe93-ae33db2d9228?version=1.0&t=1616675653756> (accessed: 17.12.2021).

⁵³ В Индексе МСЭ 2020 г. только КСА, ОАЭ и Оман достигли максимального показателя; за ними следуют государства с относительно высоким (Катар, Египет, Марокко, Тунис) и средним уровнем (Кувейт, Иордания, Бахрейн) межгосударственного сотрудничества; остальные страны (Ливия, Алжир, Сомали, Ирак, Ливан, Коморы) имеют крайне низкие и даже нулевые оценки (Джибути, Йемен, Мавритания, Палестина, Сирия, Судан). См.: GCI 2020. P. 71—82. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

⁵⁴ GCI 2020. P. 20—21. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021). Так, например, КСА ограничивается лишь двумя двусторонними соглашениями по сотрудничеству в области цифровой защиты — с ОАЭ и Великобританией. См.: Saudi Arabia // UNIDIR. March, 2021. URL: <https://unidir.org/cpp/state-pdf-export> (accessed: 20.10.2021).

Региональный тренд на востребованность активного участия внешних акторов в формировании системы безопасности (Барановский, Наумкин, 2018, с. 13; Шумилин, 2019, с. 111—117) проявляется и в сегменте цифровой защиты, как национальной, так и коллективной. На внешних треках взаимодействия представлены страны Глобального Севера (США, Великобритания, ряд государств ЕС, Республика Корея, Япония), по линии Юг — Юг партнерами арабского мира выступают Китай и мусульманские государства Юго-Восточной Азии⁵⁵.

Американское видение архитектуры коллективной киберзащиты в арабском мире, продвигаемое Вашингтоном с начала 2010-х гг., базируется на концепции создания в зоне Персидского залива субрегиональной системы безопасности, не требующей значительного присутствия США. В этой связи Вашингтон делает ставку на своих традиционных региональных союзников — КСА и ОАЭ, которых рассматривает в качестве драйверов процесса консолидации Совета сотрудничества арабских государств Персидского залива (ССАГПЗ) для совместного противостояния цифровым угрозам с последующим превращением данного объединения в интеграционное ядро общеарабской системы кибербезопасности (Alazab & Chon, 2015). Указанный подход реализуется преимущественно в рамках военного сотрудничества США с монархиями Залива и поддержки инициатив ССАГПЗ в развитии военного сегмента цифровой защиты («Киберщит полуострова» и др.⁵⁶).

⁵⁵ UNIDIR Cyber Policy Portal // The United Nations Institute for Disarmament Research. URL: <https://cyberpolicyportal.org/en/> (accessed: 10.12.2021).

⁵⁶ См.: Abedi S. Omani National Security and the Kind of Political and Military Cooperation with the United States // Modern Diplomacy. July 15, 2019. URL: <https://modern diplomacy.eu/2019/07/15/omani-national-security-and-the-kind-of-political-and-military-cooperation-with-the-united-states/> (accessed: 18.12.2021); The 5x5 — The State of Cybersecurity in the Middle East // The Atlantic Council. June 15, 2021. URL: <https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-the-state-of-cybersecurity-in-the-middle-east/> (accessed: 18.12.2021); Helou A. UAE, US Companies Partner to Provide Cyber Ranges in Gulf // C4isrnet. May 28, 2021. URL: <https://www.c4isrnet.com/industry/2021/05/28/uae-us-companies-partner-to-provide-cyber-ranges-in-gulf/> (accessed: 18.12.2021).

Китай придерживается более гибкого подхода, который также базируется на общих принципах ближневосточной политики страны, позволяющих Пекину акцентировать внимание на реализации экономических интересов, избегая при этом погружения в региональные споры (Liu, 2021). Соответственно в вопросах кибербезопасности КНР придерживается многосторонних форматов взаимодействия с арабским миром, рассматривая в качестве главной интеграционной площадки Лигу арабских государств⁵⁷ и предлагая общерегиональные проекты технологического сотрудничества в рамках инициатив «Пояса и пути» и «Цифрового Шелкового пути»⁵⁸. Приоритетными направлениями сотрудничества Китая со странами Лиги арабских государств становятся цифровая инфраструктура, финансовые технологии и онлайн-торговля⁵⁹, а с государствами ССАГПЗ, кроме того, — продвижение блокчейнов, криптовалют и иных технологий, обеспечивающих финансовую безопасность, в том числе для трансграничных платежей⁶⁰, а также технологических решений в области оптимизации государственных услуг и сокращения расточительных расходов (Mogielnicki, 2021, p. 173).

Таким образом, применительно к арабскому миру в технологическом соперничестве США и КНР достигнут определенный баланс сил, поскольку Вашингтон и Пекин преследуют

разные долгосрочные цели и используют разные методы их реализации. Более того, между двумя державами наметилось некое схожее видение обеспечения стабильности на Большом Ближнем Востоке, которое, хотя и базируется на разных исходных императивах, сводится к идее ключевого участия самих арабских стран в построении региональной системы безопасности (Liu, 2021, pp. 81, 93—94; Mogielnicki, 2021, pp. 163, 173—174). Хотя стремление ведущих внешних акторов к снижению своей вовлеченности в региональную повестку воспринимается весьма негативно в ССАГПЗ (Барановский, Наумкин, 2018, с. 13—14) и не отвечает ожиданиям ЛАГ⁶¹, оно придет импульс внутрирегиональным интеграционным процессам, в том числе в сфере кибербезопасности.

Наиболее высокая интенсивность взаимодействия в области цифровой защиты наблюдается на платформе ССАГПЗ. Схожие экономические модели и темпы развития, в том числе в цифровом сегменте, однотипность политических систем и восприятия ключевых киберугроз⁶² в совокупности с наличием общих подходов к обеспечению безопасности в зоне Залива создают благоприятные условия для формирования «единого цифрового фронта». Однако определенный технологический разрыв имеется и среди аравийских монархий, в связи с чем «отстающие» участники ССАГПЗ считают, что основной вклад в обеспечение коллективной кибербезопасности следует внести КСА и ОАЭ. Эр-Рияд и Абу-Даби со своей стороны не готовы к подобному «квотированию» обязательств во избежание излишнего давления на свой киберсектор (что чревато

⁵⁷ Wu W. China Hails Arab Data Security Pact amid Battle for Cyber Influence // South China Morning Post. March 31, 2021. URL: <https://www.scmp.com/news/china/diplomacy/article/3127795/china-hails-arab-data-security-pact-amid-battle-cyber> (accessed: 20.12.2021).

⁵⁸ Zinser S. China's Digital Silk Road Grows with 5G in the Middle East // The Diplomat. December 16, 2020. URL: <https://thediplomat.com/2020/12/chinas-digital-silk-road-grows-with-5g-in-the-middle-east/> (accessed: 18.12.2021).

⁵⁹ China, Arab League Hail Bilateral Ties, Pledge Further Cooperation // Xinhua. July 19, 2021. URL: http://www.xinhuanet.com/english/2021-07/19/c_1310069392.htm (accessed: 22.12.2021).

⁶⁰ См.: Central Banks of China and United Arab Emirates Join Digital Currency Project for Cross-Border Payments // BIS. February 23, 2021. URL: <https://www.bis.org/press/p210223.htm> (accessed: 20.12.2021); Kawate I. Thailand and UAE Join China's Global Digital Currency Push // Nikkei Asia. February 25, 2021. URL: <https://asia.nikkei.com/Business/Markets/Currencies/Thailand-and-UAE-join-China-s-global-digital-currency-push> (accessed: 22.12.2021).

⁶¹ См.: Olander E. China and the Arab League Publish Joint Statement That Showcases Beijing's Growing Geopolitical Ambitions // SupChina. July 20, 2021. URL: <https://supchina.com/2021/07/20/china-and-the-arab-league-publish-joint-statement-that-showcases-beijings-growing-geopolitical-ambitions/> (accessed: 23.12.2021); China Challenges US Position as Most Important Partner for Middle East // Business Standard. June 14, 2021. URL: https://www.business-standard.com/article/international/china-challenges-us-position-as-most-important-partner-for-middle-east-121061400348_1.html (accessed: 25.12.2021).

⁶² Cabral A.R. UAE Calls for United Front to Combat Global 'Cyber Pandemic' // The National News. November 15, 2021. URL: <https://www.thenationalnews.com/business/2021/11/15/uae-calls-for-united-front-to-combat-global-cyber-pandemic/> (accessed: 21.12.2021).

повышением уязвимости к внешним угрозам), поэтому отдают приоритет развитию национальных структур кибербезопасности, на основе которых будет строиться гибкая и устойчивая система коллективного реагирования на цифровые вызовы⁶³. Однако главным дезинтегрирующим фактором для ССАГПЗ остаются многочисленные противоречия между его участниками, выразившиеся, прежде всего, в катарском дипломатическом кризисе, а также нынешнем отсутствии единой позиции по Ирану и Израилю (Шумилин, 2019, с. 114—115; Звягельская, Свистунова, Сурков, 2020b, с. 97—98; Барановский, Наумкин, 2018, с. 14; Pradhan, 2018).

Проблемы совместной цифровой защиты стали все чаще появляться в повестке саммитов ЛАГ, причем в немалой степени под влиянием глобальных институтов, прежде всего в лице ООН⁶⁴. Общий подход Лиги к вопросам коллективной кибербезопасности еще находится в стадии разработки, но в целом предполагает, что страны с передовыми практиками, в первую очередь КСА, ОАЭ и Египет, должны оказывать арабской «цифровой периферии» помощь в формировании технического и кадрового потенциала. Арабские страны уже сделали серьезные шаги в развитии сотрудничества национальных CSIRT/CERT⁶⁵ и государственно-частного партнерства⁶⁶, подготовки кадров⁶⁷ и гармонизации профильных законодательств⁶⁸.

Вместе с тем интеграционный потенциал ЛАГ серьезно ограничивается колоссальными экономическими диспропорциями (Мельянецев, 2020; Филоник, Исаев, 2020), социально-политической фрагментацией арабских обществ (Кузнецов, 2020; Звягельская и др., 2020a; Мелкумян, 2020) и очевидным снижением интереса внешних акторов и стран ССАГПЗ к арабской периферии, цифровое развитие которой сопряжено с внушительными экономическими издержками и высокими политическими рисками⁶⁹. В этой связи в последние годы арабские страны налаживают взаимодействие без участия монархий Залива. Примерами такого сотрудничества по линии Юг — Юг могут служить обмен инновационными практиками в сфере онлайн-торговли между Египтом, Тунисом и Марокко (El-Houssami & Rizk, 2020), а также совместные мероприятия Иордании, Ливана, Алжира и Марокко по подготовке кадров⁷⁰. Однако подобные проекты, как правило, единичны, имеют узкую специализацию и не обладают достаточным интеграционным потенциалом.

Еще одной платформой взаимодействия арабских стран является ОИС, в рамках которой взаимодействуют национальные CSIRT/CERT⁷¹, функционируют Центр по противодействию кибертерроризму (создан в 2017 г.)⁷² и Рабочая группа по безопасному

⁶³ Hakmeh J., Shires J. Is the GCC Cyber Resilient? // Chatham House. March 9, 2020. URL: <https://www.chathamhouse.org/2020/03/gcc-cyber-resilient-0/summary> (accessed: 19.10.2021).

⁶⁴ Development and Harmonization of Cyber Legislation // UNCTAD. 2013. URL: https://unctad.org/system/files/non-official-document/CIEM5_ESCWA2_en.pdf (accessed: 10.10.2021).

⁶⁵ Internet Infrastructure Security. Guidelines for the Arab States // Internet Society. 2020. P. 7, 13—14. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

⁶⁶ Arab League Inks Multi-Million Dollar Deal for Regional Data Hub in Bahrain // Arab Business. September 9, 2021. URL: <https://www.arabianbusiness.com/industries/technology/468209-arab-league-inks-multi-million-dollar-deal-for-regional-data-hub-in-bahrain> (accessed: 20.12.2021).

⁶⁷ Christidis O. Technology and Youth Drive the Future of Work in MENA // Middle East Institute. October 22,

2021. URL: <https://www.mei.edu/publications/technology-and-youth-drive-future-work-mena> (accessed: 22.10.2021). См. также: (Alaleeli & Alnajjar, 2020).

⁶⁸ Hakmeh J. Cybercrime Legislation in the GCC Countries Fit for Purpose? London : Chatham House, 2018. URL: <https://www.chathamhouse.org/sites/default/files/publications/research/2018-07-04-cybercrime-legislation-gcc-hakmeh.pdf> (accessed: 22.10.2021).

⁶⁹ Ibid.

⁷⁰ См. например: Qualls: Jordan Algeria Lebanon Morocco National CTF 2020 // Cyber Talents. July 9, 2020. URL: <https://cybertalents.com/competitions/qualls-jordan-lebanon-and-morocco-national-cyber-security-ctf-2020> (accessed: 10.12.2021).

⁷¹ Online Tutoring — What It Is All about and How Much It Costs // OIC Tech Platform. September 2, 2018. URL: <http://www.oic-cert.net/> (accessed: 10.12.2021).

⁷² OIC Will Soon Establish a Cyber Security Center to Combat Cyberterrorism // OIC. November 7, 2017. URL: https://www.oic-oci.org/topic/?t_id=16023&t_ref=8082&lan=en (accessed: 10.12.2021).

использованию технологий 5G (2021 г.)⁷³, также реализуется ряд других проектов. Однако с учетом географии участников данного объединения, которая выходит далеко за пределы арабского региона, а также исключительной разнородности и противоречивости самого исламского мира, инициативы ОИС априори могут иметь самый обобщенный характер и охватывать преимущественно техническую сферу. Поэтому сотрудничество с ОИС остается важным, но не определяющим направлением интеграционных процессов в арабском мире, в том числе в области кибербезопасности.

Новый региональный тренд заложили «Соглашения Авраама» 2020 г., открывшие путь к нормализации отношений Израиля с ОАЭ и Бахрейном и ставшие кульминацией их многолетнего неофициального взаимодействия в сфере высоких технологий и кибербезопасности. Готовность Израиля и ряда арабских государств к расширению сотрудничества мотивирована идеей совместного противостояния Ирану, а также комплексом иных стратегических и коммерческих интересов⁷⁴. В сфере кибербезопасности Израиль ориентирован на кооперацию с монархиями Залива, прежде всего КСА, а также Египтом и Иорданией, с которыми активно развиваются межведомственные связи и государственно-частное партнерство, ведется разработка совместных долгосрочных программ цифрового развития, создаются двусторонние профильные рабочие группы⁷⁵. Менее продвинутые в

цифровом плане страны (Марокко, Судан), также взявшие курс на нормализацию отношений с Израилем, представляют для израильской стороны преимущественно коммерческий интерес, в связи с чем взаимодействие с ними ограничивается краткосрочными проектами⁷⁶.

Тенденция к выдвиганию Израиля на роль гаранта кибербезопасности для части арабского мира, по мнению экспертов, чревата дестабилизацией всего Ближневосточного региона как ввиду неоднозначной позиции арабских стран, в том числе государств ССАГПЗ, в отношении Ирана и Израиля, так и в свете ответного усиления наступательного киберпотенциала Ирана⁷⁷. Кроме того, по мнению обозревателей, Израиль, активно включаясь в строительство безопасной цифровой среды в ряде передовых арабских стран, рассчитывает на снижение интенсивности межарабского взаимодействия, прежде всего с враждебно настроенными к нему странами, тем самым ускоряя оттеснение на периферию слабых и/или связанных с Ираном государств (Ирака, Сирии, Йемена и др.)⁷⁸.

В целом международное сотрудничество арабских стран в сфере кибербезопасности наталкивается на те же преграды, которые ограничивают интеграционный потенциал региона. В их числе отсутствие единого экономического базиса, кризис общеарабской идентичности и свойственное всем государствам с

⁷³ Banda M. OIC-CERT Launch 5G Security Working Group at GISEC 2021 // *Intelligent CIO*. June 1, 2021. URL: <https://www.intelligentcio.com/me/2021/06/01/oic-cert-launch-5g-security-working-group-at-gisec-2021/#> (accessed: 15.12.2021).

⁷⁴ См.: El-Masry J. The Abraham Accords and Their Cyber Implications: How Iran Is Unifying the Region's Cyberspace // *Middle East Institute*. June 9, 2021. URL: <https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace> (accessed: 30.10.2021); Khorrami N. One Year On — Israel's Cybersecurity Cooperation with the GCC States // *Insights*. 2021. No. 266. P. 1—2. URL: <https://mei.nus.edu.sg/wp-content/uploads/2021/09/Insight-266-Nima-Khorrami.pdf> (accessed: 30.10.2021).

⁷⁵ Israel Is Becoming a Cybersecurity Guarantor in the Middle East // *Atlantic Council*. November 18, 2021. URL: [https://www.atlanticcouncil.org/blogs/menasource/israel-](https://www.atlanticcouncil.org/blogs/menasource/israel-is-becoming-a-cybersecurity-guarantor-in-the-middle-east-heres-how/)

[is-becoming-a-cybersecurity-guarantor-in-the-middle-east-heres-how/](https://www.atlanticcouncil.org/blogs/menasource/israel-is-becoming-a-cybersecurity-guarantor-in-the-middle-east-heres-how/) (accessed: 26.12.2021).

⁷⁶ Zainabi M. Morocco — Israel: First Steps Towards Promising Joint Projects // *The Jerusalem Post*. February 11, 2021. URL: <https://www.jpost.com/israel-news/morocco-israel-first-steps-towards-promising-joint-projects-658652> (accessed: 18.12.2021).

⁷⁷ См.: El-Masry J. The Abraham Accords and Their Cyber Implications: How Iran Is Unifying the Region's Cyberspace // *Middle East Institute*. June 9, 2021. URL: <https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace> (accessed: 30.10.2021); Khorrami N. One Year On — Israel's Cybersecurity Cooperation with the GCC States // *Insights*. 2021. No. 266. P. 1—2. URL: <https://mei.nus.edu.sg/wp-content/uploads/2021/09/Insight-266-Nima-Khorrami.pdf> (accessed: 30.10.2021).

⁷⁸ Israel Is Becoming a Cybersecurity Guarantor in the Middle East // *Atlantic Council*. November 18, 2021. URL: <https://www.atlanticcouncil.org/blogs/menasource/israel-is-becoming-a-cybersecurity-guarantor-in-the-middle-east-heres-how/> (accessed: 26.12.2021).

относительно поздней субъектностью в системе международных отношений стремление сохранить национальный суверенитет даже ценой отказа от очевидных благ кооперации (Лебедева и др., 2016, с. 23—24; Барановский, Наумкин, 2018, с. 14), в том числе в области цифровизации и киберзащиты.

Заключение

Цифровой вызов создает для арабского мира совокупность уникальных возможностей и в то же время рисков дальнейшего развития. Большинство арабских стран признали сферу ИКТ интегральной частью своих экономик и национальной безопасности. Поэтому арабский мир в целом набирает темпы в области создания киберзащиты, демонстрируя схожие с общемировыми тренды развития, но в то же время отличается разнообразием стратегий, практик и динамики продвижения

к безопасной цифровой среде. Несмотря на традиционное недоверие, в арабском мире расширяются усилия в области региональной коммуникации, имеется явное стремление к углублению регионального взаимодействия в сфере кибербезопасности там, где это уместно и продуктивно. Очевидно, что центр такого сотрудничества расположен в монархиях Залива. Однако даже там эти усилия остаются в основном реактивными и фрагментарными, а инициаторами и спонсорами объединительных процессов преимущественно выступают глобальные структуры, прежде всего в лице ООН, а также ведущие экономики мира. В целом цифровой фактор усиливает разнородность и противоречивость арабского мира, поэтому в обозримой перспективе не сможет придать необходимый импульс региональной интеграции, несмотря на наличие определенных тенденций к консолидации.

Поступила в редакцию / Received: 19.01.2022

Доработана после рецензирования / Revised: 24.02.2022

Принята к публикации / Accepted: 18.04.2022

Библиографический список

- Барановский В. Г., Наумкин В. В. Ближний Восток в меняющемся глобальном контексте: ключевые тренды столетнего развития // *Мировая экономика и международные отношения*. 2018. Т. 62, № 3 (62). С. 5—19. <https://doi.org/10.20542/0131-2227-2018-62-3-5-19>
- Звягельская И. Д., Кузнецов В. А. Государство на Ближнем Востоке: будущее началось вчера // *Международные процессы*. 2017. Т. 15, № 4 (15). С. 6—19. <https://doi.org/10.17994/IT.2017.15.4.51.1>
- Звягельская И. Д., Богачева А. С., Давыдов А. А., Ибрагимов И. Э., Самарская Л. М. и др. Политическая идентичность и ее влияние на внешнюю политику государств Ближнего Востока // *Восток. Афро-азиатские общества: история и современность*. 2020а. Т. 64, № 2. С. 55—73. <https://doi.org/10.31857/S086919080009039-9>
- Звягельская И. Д., Свистунова И. А., Сурков Н. Ю. Ближний Восток в условиях «негативной определенности» // *Мировая экономика и международные отношения*. 2020б. № 6 (64). С. 94—103. <https://doi.org/10.20542/0131-2227-2020-64-6-94-103>
- Зиновьева Е. С. Мировополитическая концептуализация международного научно-технического сотрудничества // *Вестник МГИМО-Университета*. 2018. № 6 (63). С. 242—254. <https://doi.org/10.24833/2071-8160-2018-6-63-242-254>
- Каберник В. В. Проблемы классификации кибероружия // *Вестник МГИМО-Университета*. 2013. № 2 (29). С. 72—78. <https://doi.org/10.24833/2071-8160-2013-2-29-72-78>
- Кузнецов В. А. Арабские общества эпохи неомодерна: поиск новых единств // *Восток. Афро-азиатские общества: история и современность*. 2020. № 2. С. 28—40. <https://doi.org/10.31857/S086919080009104-1>
- Кузнецов В. А. От океана до Залива: идентичность одного региона в условиях неомодерна // *Вестник Московского университета. Серия: Международные отношения и мировая политика*. 2019. № 2. С. 9—38.
- Лебедева М. М., Харкевич М. В., Зиновьева Е. С., Копосова Е. Н. Архаизация государства: роль современных информационных технологий // *Полис. Политические исследования*. 2016. № 6. С. 22—36. <https://doi.org/10.17976/jpps/2016.06.03>
- Мелкумян Е. С. Роль Лиги арабских государств в структурировании арабского регионального пространства // *Вестник МГИМО-Университета*. 2020. № 5 (13). С. 220—235. <https://doi.org/10.24833/2071-8160-2020-5-74-220-235>
- Мельянецов В. А. Долгосрочные тренды социально-экономического развития арабских стран // *Вестник МГИМО-Университета*. 2020. № 5 (13). С. 194—219. <https://doi.org/10.24833/2071-8160-2020-5-74-194-219>

- Наумкин В. В. Территориальное и демографическое «упорядочивание»: ближневосточные вызовы // Полис. Политические исследования. 2019. № 6. С. 67—80. <https://doi.org/10.17976/jpps/2019.06.06>
- Наумкин В. В. Глубоко разделенные общества Ближнего и Среднего Востока: конфликтность, насилие, внешнее вмешательство // Вестник Московского университета. Серия: Международные отношения и мировая политика. 2015. № 1. С. 66—96.
- Савельев А. Г., Карасев П. А. Перспективы регулирования и снижения военной киберугрозы // Вестник Московского университета. Серия 12: Политические науки. 2018. № 5. С. 47—61.
- Сюкияйнен Л. Р. Конституционный статус шариата как источник законодательства в арабских странах // Право. Журнал Высшей школы экономики. 2016. № 3. С. 183—205. <https://doi.org/10.17323/2072-8166.2016.4.205.222>
- Сюкияйнен Л. Р. Фикх — источник современного права в арабских странах // Право. Журнал Высшей школы экономики. 2019. № 4. С. 222—245. <https://doi.org/10.17323/2072-8166.2019.4.222.245>
- Филоник А. О., Исаев В. А. Арабский мир: слияние в нацию или усиление разобщенности? (заметки по поводу) // Азия и Африка сегодня. 2020. № 3. С. 12—19. <https://doi.org/10.31857/S032150750008723-7>
- Шумилин А. И. Ближний Восток: окно возможностей или западня для атлантистов? // Мировая экономика и международные отношения. 2019. Т. 63, № 7 (63). С. 111—120. <https://doi.org/10.20542/0131-2227-2019-63-7-111-120>
- Alaleeli S., Alnajjar A. The Arab Digital Generation's Engagement with Technology: The Case of High School Students in the UAE // *Journal of Technology and Science Education*. 2020. Vol. 10, no. 1. P. 159—178. <https://doi.org/10.3926/jotse.756>
- Alazab M., Chon S. Cyber Security in the Gulf Cooperation Council // *Social Science Research Network Electronic Journal*. 2015. P. 1—3. <https://doi.org/10.2139/ssrn.2594624>
- Alrawabdeh B. Internet and the Arab World: Understanding the Key Issues and Overcoming the Barriers // *International Arab Journal of Information Technology*. 2009. Vol. 6, no. 1. P. 27—33.
- Bunt G. *Islam in the Digital Age: E-jihad, Online Fatwas and Cyber Islamic Environments*. London and Sterling, Virginia : Pluto Press, 2003.
- Castells M. *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford, UK : Oxford University Press, 2002. <https://doi.org/10.1093/acprof:oso/9780199255771.001.0001>
- Castells M. *The Rise of the Network Society*. Vol. 1. Oxford, UK : John Wiley & Sons Ltd, 2010. <https://doi.org/10.1002/9781444319514>
- El-Houssami N., Rizk N. Innovation Practices at Makerspaces in Egypt, Tunisia and Morocco // *The African Journal of Information and Communication*. 2020. Iss. 26. P. 1—25. <https://doi.org/10.23962/10539/30357>
- Faizi I., Abubakar A. The Internet of Everything from Islamic Perspective // *International Journal on Perceptive and Cognitive Computing*. 2021. Vol. 7, no. 1. P. 66—71.
- Liu L. China's Policy and Practice Regarding the Gulf Security // *Stepping Away from the Abyss: A Gradual Approach Towards a New Security System in the Persian Gulf* / ed. by L. Narbone, A. Divsallar. San Domenico di Fiesole : European University Institute, 2021. P. 81—94. <https://doi.org/10.2870/39131>
- Mogielnicki R. Smart Context-Based Investments in the Persian Gulf's Economic Security // *Stepping Away from the Abyss: A Gradual Approach Towards a New Security System in the Persian Gulf* / ed. by L. Narbone, A. Divsallar. San Domenico di Fiesole : European University Institute, 2021. P. 163—174. <https://doi.org/10.2870/39131>
- Pöpper C., Maniatakos M., Di Pietro R. Cyber Security Research in the Arab Region: A Blooming Ecosystem with Global Ambitions // *Communications of the ACM*. 2021. Vol. 64, no. 4. P. 96—101. <https://doi.org/10.1145/3447741>
- Pradhan P. Qatar Crisis and the Deepening Regional Faultlines // *Strategic Analysis*. 2018. Vol. 42, iss. 4. P. 437—442. <https://doi.org/10.1080/09700161.2018.1482620>
- Shat F. J. F., Mousavi A., Pimenisis E. Electronic Government Enactment in a Small Developing Country — The Palestine Authority's Policy and Practice // *E-Democracy, Security, Privacy and Trust in a Digital World*. 5th International Conference. Revised Selected Papers, December 5—6, 2013. Athens, Greece : Springer International Publishing, 2013. P. 83—92. https://doi.org/10.1007/978-3-319-11710-2_8

Сведения об авторах: *Валиахметова Гульнара Ниловна* — доктор исторических наук, доцент, заведующая кафедрой востоковедения департамента (факультета) международных отношений Уральского федерального университета имени Первого Президента России Б.Н. Ельцина; ORCID: 0000-0001-7199-7723; e-mail: vgulnara@mail.ru

Цуканов Леонид Вячеславович — аспирант кафедры востоковедения департамента (факультета) международных отношений Уральского федерального университета имени Первого Президента России Б.Н. Ельцина; ORCID: 0000-0001-6882-9841; e-mail: leon.tsukanov@mail.ru

DOI: 10.22363/2313-0660-2022-22-2-320-341

Научная статья / Research article

Не конфликтом единым: потенциал цифрового взаимодействия Израиля и Палестины

С.Ю. Бабенкова¹  , Д.А. Марьясис¹ , В.М. Морозов² 

¹Институт востоковедения Российской академии наук, Москва, Российская Федерация

²МГИМО МИД России, Москва, Российская Федерация

 sbabenkova@ivran.ru

Аннотация. Ускорение процессов цифровизации, вызванное, в частности, пандемией нового коронавируса, позволяет все серьезнее рассматривать новые технологии в качестве инструмента решения ряда социально-экономических проблем как на локальном, так и на региональном и — шире — глобальном уровне. Актуальность исследования заключается в том, что сегодня и Израиль, не будучи исключением, стал участником процесса вовлечения цифровых технологий для решения государственных задач, и изучение таких возможностей может стать новым вкладом в решение палестино-израильского конфликта. Достигнутые в 2020 г. договоры о сотрудничестве Израиля с рядом арабских стран Ближнего Востока способствуют повышению степени интеграции этого государства в региональные процессы. Целью статьи является демонстрация тех возможностей, которые открывают цифровые технологии для обеспечения взаимодействия деловых сообществ Израиля и Палестины уже на современном этапе даже в условиях продолжающегося конфликта. Среди материалов, помимо совокупности научной классической апробированной литературы специалистов по Ближнему Востоку, авторы использовали научно-практические разработки в сфере экономики и антикризисного управления, что дало возможность более точной оценки ситуации и получения достоверных результатов. Использован метод декомпозиции израильско-палестинского конфликта, выделение уровней цифровизации и последующее конструирование концепции возможного использования цифрового взаимодействия между двумя странами. Результатом исследования явилась разработка многоуровневой концепции развития такого взаимодействия, основанная как на авторской трактовке процессов цифровой трансформации, так и на специфике процессов регионального развития. Центральным ее звеном являются так называемые платформы взаимодействия (ПВ), которые, по сути являясь современными онлайн-платформами, де-факто формируют виртуальное пространство для обеспечения взаимодействия двух сообществ в экономической, финансовой, образовательной, социальной сферах. Таким образом, в статье показано, что цифровизация позволяет преодолеть существующие барьеры экономического развития, особенно для Палестины, давая возможность деловому сообществу обеих стран существенно снизить значимость текущей неблагоприятной геополитической обстановки и интенсифицировать экономическую составляющую двусторонних отношений. Более того, предлагаемые нами механизмы могут действовать в условиях продолжающегося конфликта, что существенно, поскольку дают возможность постепенного улучшения экономической ситуации в Палестине.

Ключевые слова: Израиль, Палестина, цифровая трансформация, сетевая дипломатия, экономическое взаимодействие

Для цитирования: Бабенкова С. Ю., Марьясис Д. А., Морозов В. М. Не конфликтом единым: потенциал цифрового взаимодействия Израиля и Палестины // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 320—341. <https://doi.org/10.22363/2313-0660-2022-22-2-320-341>

Not a Conflict Only: Potential for Digital Interaction between Israel and Palestine

Svetlana Yu. Babenkova¹  , Dmitriy A. Mariasis¹ , Vladimir M. Morozov² 

¹Institute of Oriental Studies, Russian Academy of Sciences, Moscow, Russian Federation

²MGIMO University, Moscow, Russian Federation

 sbabenkova@ivran.ru

Abstract. The acceleration of digitalization processes, caused, in particular, by the pandemic of the new coronavirus, makes it possible to more seriously consider new technologies as a tool for solving a number of socio-economic problems, both at the local and regional and, more broadly, global levels. The relevance of the study lies in the fact that today Israel, not being an exception, has become a participant in the process of involving digital technologies to solve government problems, and the study of such opportunities can become a new contribution to the solution of the Israeli-Palestinian conflict. The agreements on cooperation between Israel and a number of Arab countries in the Middle East reached in 2020 contribute to increasing the degree of integration of this state into regional processes. The authors of the article set themselves the goal of demonstrating the opportunities that digital technologies open up to ensure interaction between the business communities of Israel and Palestine at the present stage, even in the context of the ongoing conflict. Among the materials, in addition to the collection of scientific classical proven literature of specialists in the Middle East, the authors used scientific and practical developments in the field of economics and crisis management, which made it possible to more accurately assess the situation and obtain reliable results. Among the methods, the authors used the method of decomposition of the Israeli-Palestinian conflict, the allocation of levels of digitalization and the subsequent construction of the concept of the possible use of digital interaction between the two countries. The result of the study was the development of their own multi-level concept for the development of such interaction, based both on their understanding of digital transformation processes and on the specifics of regional development processes. The central element of the concept developed by the authors of the article is the so-called interaction platforms (IP), which, in fact, being modern online platforms, de facto form a virtual space to ensure the interaction of the two communities in the economic, financial, educational, and social spheres. Thus, the article shows that digitalization makes it possible to overcome the existing barriers to economic development, especially for Palestine. It enables the business community of both countries to considerably reduce the significance of the current unfavorable geopolitical situation and intensify the economic component of bilateral relations. Moreover, the mechanisms we propose can operate in the context of an ongoing conflict, which is of paramount importance, since in this case there is a possibility of a gradual improvement in the economic situation in Palestine.

Key words: Israel, Palestine, digital transformation, network diplomacy, economic interaction

For citation: Babenkova, S. Yu., Mariasis, D. A., & Morozov, V. M. (2022). Not a conflict only: Potential for digital interaction between Israel and Palestine. *Vestnik RUDN. International Relations*, 22(2), 320—341. (In Russian). <https://doi.org/10.22363/2313-0660-2022-22-2-320-341>

Введение

Палестино-израильский конфликт является одним из самых длительных в современной истории и проходит «красной нитью» по истории Ближнего Востока. На протяжении долгого времени международные лидеры, дипломаты, ученые обсуждали возникшие в ходе противостояния двух народов проблемы и пытались найти выходы из сложившейся

ситуации. В последние несколько десятилетий мир сильно изменился, и проблемы безопасности, в том числе экономической и информационной, стоящие перед странами Ближнего Востока, вышли на первый план. В попытках прийти к решению были задействованы и финансовые ресурсы, но, несмотря на миллиарды долларов, потраченные на поддержку противоборствующих сторон, противодействие конфликту или попытки его урегулирования,

конфликт продолжается уже в течение десятилетий с периодическими вспышками насилия. Каждая такая вспышка приводит к падению ВВП Палестины на душу населения примерно на 46 %, в то время как ВВП Израиля на душу населения падает примерно на 10 %¹. Взяв за основу то, что взаимовыгодная экономическая деятельность может повысить интерес к мирному урегулированию конфликта, представляется целесообразным рассмотреть противостояние с данной точки зрения.

Конечно, многие вопросы и проблемы остаются неразрешимыми. При этом целесообразно отметить, что в обеих странах существует большой интеллектуальный человеческий потенциал, который поможет эффективно использовать возможности инновационной экономики XXI в. и, возможно, принесет новые неожиданные варианты мирного разрешения конфликта. Речь, в первую очередь, идет о несиловых методах разрешения конфликта, связанных с так называемой «мягкой силой», инструментами и механизмами сетевой дипломатии (Морозов, Шебалина, Лебедева, 2019).

За десятилетия изучения палестино-израильского противостояния было выдвинуто множество предложений и идей по его разрешению, однако эти планы не были реализованы, в том числе из-за того, что их цели и задачи полностью или частично не удовлетворяли ни одну из сторон конфликта и не учитывали быстро меняющиеся реалии Ближневосточного региона (Федорченко, Крылов, Морозов, 2018, с. 5—20).

Вместе с тем страны Востока в последние десятилетия достаточно активно включены в процесс тех фундаментальных изменений, затрагивающих все сферы жизни, которые в экономической литературе часто называют четвертой промышленной революцией². Изменяются структуры национальных хозяйств — явления, которые привлекают как

отечественных, так и иностранных исследователей³. Цифровизация в этих процессах играет существенную роль (Коровкин, 2019; Бабенкова, 2019).

Авторы статьи не ставили перед собой задачу создать «универсальный и быстродействующий» механизм решения многолетнего конфликта. Данная статья — попытка предложить систему организации взаимовыгодного сосуществования двух народов в экономической сфере в ситуации, когда палестино-израильский конфликт не решен. Мы рассмотрели и проанализировали возможные точки соприкосновения двух государств в сфере взаимодействия в области цифровой экономики и как действенного инструмента преодоления экономических проблем, связанных с продолжающимся конфликтом, и как нового инструмента преодоления части существующих проблем в экономике каждой из его сторон.

События 2020 г. при всей их драматичности привели к двум, на наш взгляд, существенным изменениям как в мире в целом, так и в регионе в частности, что делает результаты исследования особенно актуальными.

Во-первых, пандемия нового коронавируса привела к беспрецедентному росту цифровизации не только в сфере управления государством и деловой среде, но и в частной жизни. Огромные массы населения были вынуждены «вступить в цифровой мир», чтобы обеспечить себе минимальный уровень безопасности и комфорта. Процессы цифровой трансформации существенно интенсифицировались на глобальном уровне, охватив все аспекты жизнедеятельности человека, — от доставки продуктов питания до получения медицинской помощи и организации досуга (в том числе культурного); корпоративная культура также существенно преобразилась. Даже после изменения ситуации с коронавирусом в лучшую сторону вряд ли следует ожидать резкого сокращения использования цифровых технологий: скорее, наоборот, период пандемии послужил катализатором необратимого процесса цифровизации.

³ См., например: (Schroeder, 2013; Новая система производительных сил..., 2019).

¹ Ross A.C. et al. The Costs of the Israeli-Palestinian Conflict. Santa Monica, CA: RAND Corporation, 2015. URL: https://www.rand.org/pubs/research_reports/RR740-1.html (accessed: 23.02.2022).

² Об этом явлении см., например: (Шваб, 2020).

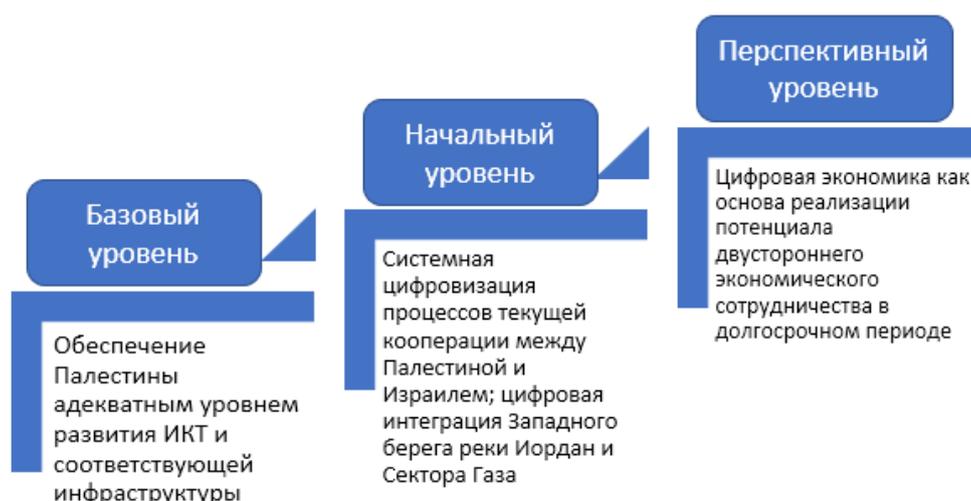


Рис. 1. Развитие палестино-израильского сотрудничества в области цифровизации
 Источник: разработано авторами.

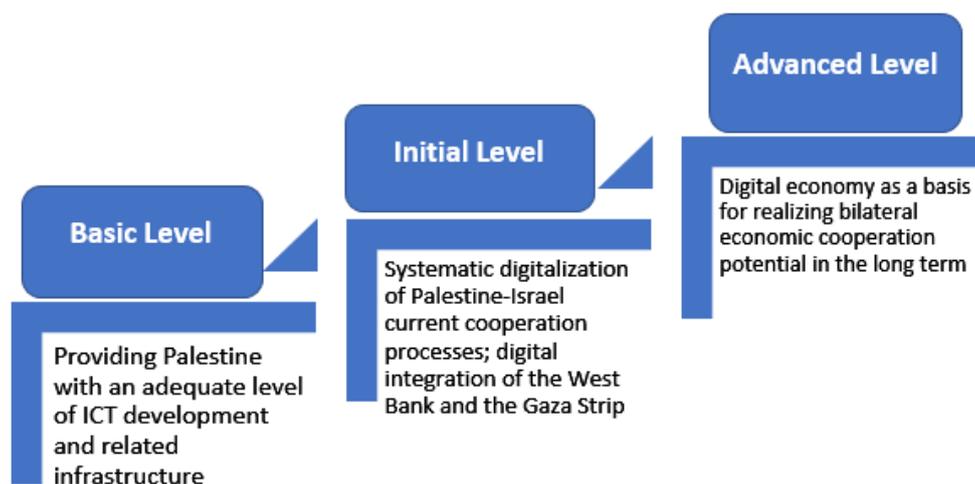


Fig. 1. Palestine — Israel Cooperation Development in the Field of Digitalization
 Source: compiled by the authors.

Во-вторых, осенью-зимой 2020 г. были подписаны договоры о нормализации отношений Израиля с Объединенными Арабскими Эмиратами (ОАЭ), Бахрейном, Суданом и Марокко. Подписание этих так называемых «Авраамовых соглашений» свидетельствует о коренном изменении геополитической обстановки в Ближневосточном регионе (Ахматшина, Лиокумович, 2022, с. 64—68). В контексте нашей работы в лице этих арабских стран (особенно ОАЭ) появляется новый финансово состоятельный игрок, как заинтересованный в снижении уровня палестино-израильского противостояния в целом, так и готовый активно содействовать экономическому развитию Палестины как идеологически

важной составляющей арабского мира. Активное развитие цифровой экономики в ОАЭ и Бахрейне — это один из существенных факторов, позволяющих нам считать сделанные в данной работе концептуальные предложения актуальными.

Без интенсификации процесса цифровизации экономик Израиля и Палестины сложно говорить о перспективах развития национальных хозяйств этих государств в долгосрочном периоде. Причем для Палестины этот процесс обладает существенно большей важностью, так как позволяет преодолеть ряд текущих существенных (если не сказать жизненно важных) проблем ее хозяйственного развития.

На рис. 1 представлена предлагаемая авторами концепция трехуровневой двусторонней кооперации в области цифровой экономики.

Далее целесообразно остановиться на каждом из уровней. Мы также рассмотрим и предложим концептуализацию антикризисной роли инструментов цифровой экономики.

Развитие информационно-коммуникационных технологий в Палестине

Начнем с более подробного рассмотрения того, что можно назвать базовым уровнем сотрудничества в области цифровизации между Палестиной и Израилем, а именно — развития кооперации двух стран по обеспечению Палестины адекватным уровнем информационно-коммуникационных технологий (ИКТ) и соответствующей инфраструктуры⁴. Очевидно, что, во-первых, без этого в современном мире любой экономике развиваться невозможно, а, во-вторых, без активного участия Израиля палестинцам будет невозможно преодолеть отставание в процессе развития ИКТ на своей территории.

Цифровая экономика для Палестины может стать необходимой поддержкой для экономического роста, в том числе в части создания новых рабочих мест в условиях роста населения и большого процента трудоспособной безработной молодежи. Несмотря на кажущуюся парадоксальность данного заявления ввиду того, что цифровизация ведет к замене человеческого труда машинным, оно абсолютно логично, так как цифровая инфраструктура позволит упростить открытие нового бизнеса, а повышение уровня взаимодействия с Израилем через соответствующие платформы позволит палестинским деловым структурам напрямую работать с израильскими компаниями. Конечно, проблемы

⁴ Фактологическая информация, если не указано иное, приведена на основе: Economic Monitoring Report to the Ad Hoc Liaison Committee // The World Bank. June 2, 2020. URL: <http://documents1.worldbank.org/curated/en/844141590600764047/pdf/Economic-Monitoring-Report-to-the-Ad-Hoc-Liaison-Committee.pdf> (accessed: 17.07.2021).

внедрения цифровых инфраструктур в Палестине обусловлены прежде всего ограничениями по перемещению людей и товаров. В этой связи варианты развития сектора инновационных технологий рассматриваются с учетом взвешенных рисков.

Палестина занимает 123-е место в мире в области ИКТ, что значительно ниже среднего уровня по сравнению с другими арабскими государствами. На Палестинских территориях проживает примерно 4,8—5 млн человек, среди которых значителен процент безработной молодежи. При этом, по состоянию на 2019 г., в стране насчитывалось 3000 выпускников высших учебных заведений по направлениям: инжиниринг, математика, технологии, ИКТ⁵. По нашему мнению, это хороший кадровый потенциал для компаний, которые хотят выйти на рынок инновационных технологий.

Исходя из вышеизложенного, у страны возникает острая необходимость сократить отставание в цифровом развитии по отношению к другим странам региона. В этой связи часть палестинской программы «Повестка для XXI века», названная «Граждане на первом месте (2017—2022 гг.)»⁶, определяет цифровую трансформацию социально-экономических и финансовых секторов в качестве приоритетных направлений для достижения устойчивости экономики в условиях постоянных внешнеполитических вызовов⁷. Сектор ИКТ в Палестине составляет 7 % от ВВП⁸, однако спрос на цифровизацию своей деятельности может родиться у таких

⁵ См., в частности, данные: Goichman R. Palestinian High-tech Workers Plugging Shortage of Israeli Tech Staff // Haaretz. July 4, 2018. URL: <https://www.haaretz.com/israel-news/business/palestinian-high-tech-workers-plugging-shortage-of-israeli-tech-staff-1.6243852> (accessed: 23.02.2022).

⁶ National Policy Agenda 2017—2022 — Putting Citizens First // ESCWA. January 2016. URL: <https://andp.unescwa.org/plans/1216> (accessed: 23.02.2022).

⁷ Economic Monitoring Report to the Ad Hoc Liaison Committee // The World Bank. June 2, 2020. URL: <http://documents1.worldbank.org/curated/en/844141590600764047/pdf/Economic-Monitoring-Report-to-the-Ad-Hoc-Liaison-Committee.pdf> (accessed: 17.07.2021).

⁸ Ibid.

направлений, как сельское хозяйство, здравоохранение, образование, государственные услуги.

Для появления динамично развивающейся и безопасной цифровой экономики в Палестине официальным властям страны необходимо развивать цифровую инфраструктуру, в том числе универсальный, доступный и широкополосный Интернет⁹, который является основой жизнедеятельности цифровой экономики, но из-за многочисленных внутринациональных и двусторонних проблем маловероятно, что уровень проникновения Интернета в Палестине к 2030 г. достигнет отметки 20 %¹⁰, достаточной для достижения универсального доступа к широкополосному Интернету хорошего качества. Отметим, что на конец 2018 г. уровень проникновения широкополосной связи в Палестине был на отметке 5,39 %, что являлось самым низким показателем в регионе Ближнего Востока и Северной Африки (БВСА). На 100 человек населения приходилось 8 пользователей широкополосной связью¹¹. Услуги связи предоставляются Палестинской телекоммуникационной компанией (PalTel) посредством DSL¹², при этом

⁹ Для подключения большого количества пакетов цифровых продуктов и услуг.

¹⁰ В 2018 г. руководство Всемирного банка решило внедрить в странах БВСА инициативу по достижению полного охвата широкополосного Интернета в регионе к 2030 г. См.: Economic Monitoring Report to the Ad Hoc Liaison Committee // The World Bank. June 2, 2020. URL: <http://documents1.worldbank.org/curated/en/844141590600764047/pdf/Economic-Monitoring-Report-to-the-Ad-Hoc-Liaison-Committee.pdf> (accessed: 17.07.2021). Для сведения: по состоянию на конец 2019 г. в России уровень проникновения Интернета находился на отметке в 76 %. Приводится по: Сергеева Ю. Вся статистика Интернета на 2019 год – в мире и в России // Web Canape. 11.02.2019. URL: <https://www.web-canape.ru/business/vsya-statistika-interneta-na-2019-god-v-mire-i-v-rossii/> (дата обращения: 23.07.2021).

¹¹ Сергеева Ю. Вся статистика Интернета на 2019 год – в мире и в России // Web Canape. 11.02.2019. URL: <https://www.web-canape.ru/business/vsya-statistika-interneta-na-2019-god-v-mire-i-v-rossii/> (дата обращения: 23.07.2021).

¹² Означает «Цифровая абонентская линия», является средством связи, используемым для передачи цифровых сигналов по стандартным телефонным линиям.

стоимость услуг в секторе Газа и на Западном берегу различаются.

Несмотря на то, что в рамках существующих соглашений Палестина имеет право строить и эксплуатировать свою независимую телекоммуникационную инфраструктуру и устанавливать правовые нормы в области информационно-коммуникационной политики, Израиль принимает решения относительно спектра выделенных частот. Палестинские операторы сталкиваются с ограничениями со стороны Израиля по строительству вышек и прокладке сетей, а также не выдерживают конкуренции с израильскими сотовыми операторами, которые могут предложить связь 4G и контролируют 20 % рынка широкополосного Интернета на Западном берегу¹³.

В настоящее время 99 % населения Палестины имеет доступ к мобильной связи и сетям 2G (в 2019 г. прирост составил 73 %), при этом 52 % населения доступны и сети 3G (к концу 2019 г. прирост составил 12 %). За последние 5 лет на 40 % увеличилось количество использования интернет-трафика, при этом 67 % населения имеет доступ к всемирной паутине¹⁴.

Учитывая определенное отсутствие фиксированной широкополосной инфраструктуры, Палестина старается внедрить подключение мобильных услуг широкополосной связи через точки доступа Wi-Fi. Рынок мобильной широкополосной связи более конкурентоспособен в стране, чем рынок фиксированной широкополосной связи. Мобильная широкополосная связь представлена двумя операторами — Jawwal (дочерняя компания PalTel) и Ooredoo Palestine (бывшая Wataniya Mobile Palestine). В начале 2018 г. эти две компании развернули сети 3G после выделения Израилем соответствующих частот доступа к национальной сети мобильной широкополосной связи. В секторе Газа доступ к 3G палестинским провайдерам закрыт, однако из-за

¹³ Economic Monitoring Report to the Ad Hoc Liaison Committee // The World Bank. June 2, 2020. URL: <http://documents1.worldbank.org/curated/en/844141590600764047/pdf/Economic-Monitoring-Report-to-the-Ad-Hoc-Liaison-Committee.pdf> (accessed: 17.07.2021).

¹⁴ Ibid.

близости Израиля палестинцы могут получать сигнал и пользоваться сетями 3G и 4G/LTE от израильских операторов. Аналогичная ситуация происходит и на Западном берегу.

На сегодняшний день дефицит диапазона частот для предоставления широкополосной качественной связи сказывается в первую очередь на потребителях услуг, так как узкая полоса пропускания сигнала приводит к удорожанию развертывания оборудования ретрансляционных станций в связи с увеличением мощностей для решения проблем дополнительных нагрузок (растущим трафиком). Целесообразно также отметить ограниченное количество абонентов, которых может обслуживать оператор мобильной связи, и высокую себестоимость трафика для этих абонентов. Увеличивающийся спрос на сети 4G и в будущем 5G приведет к нагрузке на коммуникационный сектор Палестины, который не имеет полноценной возможности справиться с этой проблемой без помощи соседнего Израиля.

Однако широкому развитию цифровой инфраструктуры мешают не только нерешенные проблемы палестино-израильских взаимоотношений, но и отсутствие в Палестине актуальной нормативно-правовой базы, регламентирующей деятельность объектов цифровой инфраструктуры. Сектор телекоммуникаций регулируется Законом № 3 от 1996 г. «О телекоммуникациях»¹⁵ и не учитывает актуальные стратегии, которые существуют в цифровой экономике и ИКТ.

С 2005 г. палестинское Министерство телекоммуникаций и информационных технологий (далее — МТ и ИТ) занимается актуализацией нормативно-правовой базы в соответствии с международной практикой и стандартами, принятыми в данной области, а также планирует создать независимую палестинскую Службу по надзору в сфере связи. Политическая нестабильность помешала Службе

начать осуществлять свою деятельность в 2010 г. и, по имеющимся у авторов сведениям, к моменту подготовки данной статьи работать она так и не начала.

Какой инструментарий сможет помочь расширить доступ к недорогой и качественной широкополосной связи в Палестине и ускорить рост сектора ИКТ? Конечно, необходимо «реанимировать» работу Объединенного технического комитета¹⁶ для проведения оперативных совещаний и рабочих встреч в двустороннем палестино-израильском формате с целью выработки единой концепции по развитию телекоммуникационного сектора в Палестине, который будет сопоставим по надежности и качеству предоставляемых услуг с другими странами региона. Видятся целесообразными следующие действия:

— установление согласованных и разумных сроков предоставления палестинским операторам частот для использования 4G, а в конечном итоге 5G, исходя из запросов палестинского мобильного рынка;

— уменьшение «эффекта присутствия» израильских телекоммуникационных компаний на Западном берегу (использование микроячеек с меньшим радиусом покрытия вместо использования макроячеек);

— внесение изменений в положения, касающиеся ограничений при применении ИКТ. Палестинские компании смогут работать эффективно, если будут внедрять инновационные технологии, а также будет осуществлено принятие всеми заинтересованными в налаживании взаимодействия сторонами подходов к поставкам импортного оборудования, основанных на оценке риска его использования в коммерческих целях, а не для подрыва безопасности соседних стран;

— обеспечение Израилем доступа к инфраструктуре и участкам земли в зоне «С» для установки оборудования и предоставления услуг связи палестинскому населению;

¹⁵ The Telecommunication Sector in the Palestinian Territories: A Missed Opportunity for Economic Development // The World Bank Group. January 2, 2016. URL: <https://openknowledge.worldbank.org/bitstream/handle/10986/24019/104263.pdf?sequence=5> (accessed: 23.02.2022).

¹⁶ Объединенный технический комитет был создан в 1994 г. после Соглашения в Осло как техническая, а не политическая платформа по рассмотрению вопросов двусторонних отношений в телекоммуникационной сфере, однако его заседания ни разу не проводились.

— рассмотрение возможности создания национальной волоконно-оптической магистрали с привлечением мощности Электрической компании района Иерусалима (JDECO). Палестинские территории являются одними из самых густонаселенных районов (800 чел. на кв. км) с наименьшей территорией¹⁷. Учитывая быстрый рост, популярность и, как следствие, уменьшение стоимости оптических волокон, плотность населения и незначительные территории, которые есть у Палестины, позволяют строить комплексную наземную оптико-волоконную инфраструктуру.

Здесь целесообразно отметить, что JDECO уже оборудовал более 400 км распределительной сети в Иерусалиме, Рамаллахе, Иерихоне и Вифлееме¹⁸. Оптико-волоконная сеть широко используется для функционирования силовых подстанций, имеет более высокие характеристики по качеству и скорости связи и передачи информации, которые могут предоставляться потребителям в виде продуктов и услуг по более гибким ценам, чем мобильный Интернет.

Наряду с вышесказанным необходимо обратить внимание на разработку недорогих, широкополосных беспроводных технологий, в частности на производителей оборудования, технологий (новых стандартов) беспроводной локальной сети Wi-Fi, число которых в мире растет. В Палестине очень хорошо развиваются стартапы, в том числе среди молодых специалистов. В этой связи рынок Wi-Fi особенно подходит для апробации новых стандартов передачи цифровых потоков, исключая наложенные израильской стороной ограничения.

В краткосрочном периоде также необходимо продолжить работы по созданию независимой палестинской Службы по надзору в сфере связи и по обновлению и апробации нормативно-правовой базы в области ИКТ, а также принять новый Стратегический план по

цифровой экономике для Палестинских территорий, так как потребность в цифровой экономике растет, а последний Стратегический план, в котором даны понятие и определение электронного правительства, был принят в 2005 г. и морально устарел и не подходит под новые реалии.

Цифровизация для обеспечения текущих процессов палестино-израильской коммуникации и интеграции обеих частей Палестины

На сегодняшний день, несмотря на все геополитические проблемы, две территории достаточно активно взаимодействуют друг с другом: палестинские рабочие едут на работу в Израиль и обратно, с территории Палестины в Израиль поступают определенные товары, товары также поступают в Палестину через израильские проверяющие органы, осуществляется трансфер финансовых средств, в Палестину въезжают иностранные бизнесмены, туристы, официальные лица. Для контроля всех указанных потоков соответствующие органы Израиля и Палестины вынуждены коммуницировать, хотя бы они того или нет.

Представляется, что цифровизация всех указанных процессов позволит существенно повысить их эффективность и прозрачность. Приведем несколько примеров. Так, возможность электронной записи для пересекающих КПП граждан Палестины с сохранением в виртуальном облаке всей необходимой про них информации (личные и контактные данные, время и места предыдущих пересечений границы, других важных для системы израильской безопасности данных) позволило бы не только ускорить сам процесс, но и сделать его в принципе более комфортным для палестинцев. Повысилась бы и степень прозрачности данного процесса.

Перевод всей системы контрактования палестинских работников в киберпространство позволяет не только повысить прозрачность и эффективность этой сферы (иначе много повторений), но и дает возможность работникам вести все свои финансовые операции онлайн, по крайней мере на территории

¹⁷ Economic Monitoring Report to the Ad Hoc Liaison Committee // The World Bank. June 2, 2020. URL: <http://documents1.worldbank.org/curated/en/844141590600764047/pdf/Economic-Monitoring-Report-to-the-Ad-Hoc-Liaison-Committee.pdf> (accessed: 17.07.2021).

¹⁸ Ibid.

Израиля. Более того, в среднесрочной перспективе возникает потенциал появления палестино-израильской криптовалюты. Она может заменить израильский шекель в расчетах между израильскими работодателями и палестинскими работниками. Поскольку криптовалюта сама является финансовым активом, палестинцы смогут ею торговать с использованием соответствующих инструментов.

Если же исходить из того, что введение криптовалюты — слишком амбициозная цель на ближайшую перспективу, то представляется релевантным возвращение к идее создания палестинской валюты, которая соответствовала бы Парижскому протоколу и международному праву. Это наделит палестинскую экономику рядом преимуществ: снижение издержек обмена валют; обеспечение того, что доход государства от выпуска бумажных денег, не имеющих собственной стоимости (разница между номиналом и стоимостью изготовления), оставался бы в Палестине; стимулирование большей экономической гибкости. Это позволит Палестинскому валютному управлению (РМА) стать центральным банком, главной инстанцией для банковского сектора, который также мог бы вкладывать средства непосредственно в экономику. Такие расходы не были бы инфляционными, если бы они позволяли неиспользуемым производственным мощностям и многочисленным безработным палестинцам создавать новые товары и услуги.

Возвращаясь к прорывным тенденциям в цифровизации, развитие блокчейн-технологий позволит трансформировать логистику поступления и вывоза из Палестинской национальной администрации (ПНА) товаров. Цифровизация — это мощнейший инструмент повышения степени прозрачности рынка. Так, у палестинцев появится возможность контролировать доставку и реагировать на нарушения процесса, в том числе со стороны израильских властей. Вместе с тем израильские контролирующие органы получают возможность тратить меньше ресурсов на отслеживание грузопотока и сконцентрироваться на ситуациях, которые могут иметь отношение к контрабанде и терроризму (например,

попытка провоза товаров без использования одобренной обеими сторонами системы определения происхождения и пр.).

Одной из самых серьезных проблем Палестины является ее географическая раздробленность. Как ни соединяй Западный берег с сектором Газа при помощи туннеля или моста, все равно разрыв будет ощущаться. Цифровая экономика является одним из эффективных инструментов решения территориальной проблемы. Об этом, в частности, много говорят в Израиле. Цифровые ресурсы — даже самые простые — позволят, во-первых, международно признанному руководству Палестины повысить степень своего контроля над всей ее территорией через социальные выплаты, соответствующее информирование, организацию общественных процессов (от культурных мероприятий до выборов), а во-вторых, непосредственно жителям обеих территорий станет проще организовать разного рода взаимодействие между собой.

У авторов нет сомнения в том, что даже для реализации цифровизации на таком достаточно простом по современным меркам уровне требуется решить как минимум две очень серьезные задачи:

1) принять соответствующие политические решения (причем принять их должны власти обеих стран);

2) обеспечить финансирование создания соответствующих инструментов.

По нашему мнению, обе вышеуказанные задачи определенно решаемы уже в краткосрочном периоде. Основные решения можно согласовать в рабочем порядке — необходимости проводить двусторонние встречи на высшем уровне (что в момент написания работы крайне затруднено) нет, а руководство каждой из сторон потом может обеспечить необходимую политическую поддержку самостоятельно. Финансирование реализации особенно на начальном этапе, скорее всего, по крайней мере в части палестино-израильской кооперации, будет вынужден взять на себя Израиль. Однако, как кажется, вложения если и не окупятся в прямом смысле, то опосредованная выгода от возникновения описанной системы цифровой кооперации может быть существенной.

Подчеркнем, что ускорение процессов цифровой трансформации, вызванное пандемией нового коронавируса, в любом случае в итоге так или иначе будет способствовать формированию новой реальности и на Ближнем Востоке.

Цифровая экономика как возможность нового уровня кооперации между Палестиной и Израилем

В начале 1990-х гг., когда мирный процесс на Ближнем Востоке набирал обороты, у ряда представителей израильской политической и экономической элиты возникло ощущение, что израильско-палестинское сотрудничество в экономической сфере может стать фундаментом долгосрочного позитивного взаимодействия между двумя народами¹⁹. Однако уже к началу XXI в. стало понятно, что, к сожалению, во многом такие надежды иллюзорны²⁰. При этом все же экономическое сотрудничество между Израилем и Палестиной продолжалось. Существует оно и в конце второго десятилетия нынешнего столетия. Несмотря на то, что самой известной формой двусторонней кооперации является (в основном) низкоквалифицированный труд палестинских рабочих в израильских сельскохозяйственных и строительных компаниях, этим она не ограничивается.

В рамках статьи авторы не будут подробно останавливаться на рассмотрении конкретных кейсов палестино-израильского делового сотрудничества. Отметим лишь, что в большинстве своем оно не носит системного характера и вряд ли его можно считать нацеленным на долгосрочную перспективу. При этом важно указать на то, что в Израиле действуют несколько проектов, нацеленных на оказание системного содействия экономическому развитию Палестины.

Самым известным является палестинское направление деятельности Центра по международному сотрудничеству, известного как МАШАВ²¹. В рамках данного направления

МАШАВ сосредоточивает свои усилия, помимо прочего, на развитии сельскохозяйственного направления в Палестине и стимулировании усиления роли женщин и молодежи в экономической сфере жизни палестинского общества.

С точки зрения рассматриваемых в данной статье вопросов наибольший интерес вызывает проект *Palestinian Internship Program* (PIP)²², направленный на содействие палестинским специалистам в получении практики в израильских компаниях технологического сегмента национальной экономики. К 2020 г. созданная в 2014 г. в США (создатель — американско-израильский предприниматель Ядин Кауфман) программа позволила 67 палестинцам получить практику в 43 израильских технологических компаниях. 35 % из практикантов остались работать в израильских компаниях, а еще порядка 33 % вернулись в ПНА на руководящие должности²³. Однако это «капля в море»: ежегодно палестинские университеты выпускают порядка 2,5—3 тыс. технических специалистов, которым в современных условиях крайне сложно найти адекватную работу или создать свой технологический бизнес в Палестине²⁴.

Нельзя также не отметить начавший работать в 2017 г. проект *Tech2Peace*, основная идея которого состоит в том, чтобы способствовать разрешению палестино-израильского

развитию. Занимается проведением ряда тренингов и других обучающих программ по использованию эффективных методов развития различных отраслей хозяйства. Сельское хозяйство здесь зачастую играет главную роль. В определенной степени эта программа является скрытой рекламой израильских технологий. Подробнее о программе МАШАВ см.: (Якимова, 2019, с. 97—108).

²² См. официальный сайт проекта: *Palestinian Internship Program*. URL: <https://www.palinternship.com/> (accessed: 23.07.2021).

²³ Yablonko Y. Intern Program Boosts Palestinian Tech Sector // *Globes*. March 4, 2020. URL: <https://en.globes.co.il/en/article-intern-program-boosts-palestinian-tech-sector-1001320552> (accessed: 23.07.2021).

²⁴ Palestine — Technology for Youth and Jobs Project (TechStart) // DAI. URL: <https://www.dai.com/our-work/projects/palestine-technology-for-youth-and-jobs-project-techstart> (accessed: 27.03.2022).

¹⁹ См., в частности: (Перес, 1994).

²⁰ См., в частности: (Марьясис, 2003, с. 27—32).

²¹ МАШАВ (ивр. Merkaz le shituf peula beinleummi) — Центр содействия экономическому

конфликта через технологическое образование²⁵. В рамках проекта организуются серии тренингов, мастер-классов, а также групп обсуждения. Все мероприятия посещают смешанные группы израильской и палестинской молодежи. Тренинговые форматы посвящены непосредственно технологическому образованию — 3D-моделированию, разработке приложений и другим актуальным темам технологического развития. Они призваны дать молодежи (особенно палестинской) необходимые навыки для дальнейшего развития в рамках современной основанной на высоких технологиях экономики. Наряду с этим в группах обсуждения молодые люди дискутируют по вопросам, связанным с проблемой разрешения палестино-израильского конфликта.

Исходя из существующих экономических проектов, направленных на мирное урегулирование конфликта, Израилю и Палестине необходимо наращивать соответствующие усилия и укреплять экономические связи. Еще в 2008 г. в своей предвыборной кампании Биньямин Нетаньяху подчеркнул: «Мы должны достичь экономического мира наряду с политическим. Это означает, что нам следует укрепить экономический потенциал части палестинской экономики, не нацеленной на противоборство, и обеспечить ее быстрый рост, что принесет мир для рядовых палестинцев»²⁶.

В настоящее время помощь международного сообщества является спасательным кругом Палестинской администрации. К 2008 г. на международную помощь приходилось более 60 % валового национального дохода Палестины. Для сравнения корпорация RAND подсчитала, что в случае мирного разрешения конфликта обе стороны получают значительную выгоду как в абсолютном выражении,

так и в ВВП на душу населения²⁷: в то время как доход среднего израильца увеличился бы примерно на 2250 долл. США (около 5 %), доход среднего палестинца вырос бы примерно на 1 100 долл. США (около 36 %) (Cohen, 2013, pp. 132—150).

Среди крупнейших и наиболее успешных экономических инициатив — совместные промышленные парки, инициатива «Долина мира», «Оливки мира» (совместное израильско-палестинское предприятие по продаже оливкового масла). В то время как индустриальные парки и инициатива «Долина мира» являются проектами, поддерживаемыми правительством и создающими рабочие места в Израиле и на Западном берегу реки Иордан, сторонам необходимо двигаться дальше в направлении партнерства частных компаний. Некоторая напряженность возникла вокруг существующих правительственных экономических проектов. Одним из примеров было создание Раваби, нового города, в строительстве которого частично помог Израиль. На первом этапе там предполагалось разместить 40 000 человек, а в будущем — еще больше; первые 700 домов были построены уже к 2015 г.²⁸ Однако конфликты с израильскими властями не позволили создать автомагистраль (была построена лишь только однополосная фермерская дорога), также не были решены проблемы с доступом к воде.

В 2016 г. в ходе официального визита в Израиль тогдашний госсекретарь США Джон Керри заявил, что улучшение экономической ситуации создаст благоприятную среду для политического прогресса, в то время как восстановление экономики поможет создать атмосферу доверия между двумя сторонами²⁹. Существует потребность в инициативах,

²⁷ Ross A.C. et al. The Costs of the Israeli-Palestinian Conflict. Santa Monica, CA: RAND Corporation, 2015. URL: https://www.rand.org/pubs/research_reports/RR740-1.html (accessed: 23.02.2022).

²⁸ Ibid.

²⁹ Full Text: John Kerry's Remarks on Middle East Peace // Politico. December 28, 2016. URL: <https://www.politico.com/story/2016/12/full-text-john-kerry-2016-israel-mideast-peace-speech-transcript-233014> (accessed: 02.03.2022).

²⁵ Sheidlower N. Tech2Peace Brings Together Palestinians, Israelis through Tech and Dialogue Workshops // NoCamels. August 20, 2020. URL: <https://nocamels.com/2020/08/tech2peace-palestinians-israelis-tech-dialogue/> (accessed: 01.09.2021).

²⁶ Ahren R. Netanyahu: Economics, Not Politics, Is the Key to Peace // Haaretz. November 20, 2008. URL: <https://www.haaretz.com/1.5061173> (accessed: 24.08.2021).

предполагающих сельскохозяйственные, промышленные, туристические и совместные проекты в дополнение к центрам занятости вблизи крупных городов, которые позволят палестинцам отказаться от работы на территории Израиля, облегчат транзит через контрольно-пропускные пункты и привлекут иностранные инвестиции (Seidel & Abu-Nimer, 2015, p. 559).

Свою деятельность ведут также различные неправительственные организации (НПО), которые стремятся содействовать экономическому партнерству между израильскими и палестинцами (например, Израильско-Палестинская торгово-промышленная палата, Фонд экономического сотрудничества (ECF) и др.). Как правительствами, так и частными корпорациями предпринимались разнообразные попытки оформить экономическое сотрудничество Израиля и Палестины, поскольку экономический базис является, возможно, самой надежной гарантией сохранения мира.

Очевидно, что геополитическая ситуация не позволяет в полной мере реализовать возможный потенциал палестино-израильского делового взаимодействия. Однако развитие инновационной экономики и происходящая в обеих странах цифровая трансформация позволяют посмотреть на перспективы сотрудничества под другим углом. Далее в работе авторы подробнее рассмотрели некоторые возможные варианты преодоления существующих барьеров при помощи цифровых технологий. Другими словами, в данной части статьи авторами рассмотрен перспективный уровень двустороннего сотрудничества в области цифровой трансформации (см. рис. 1).

Виртуальные кластеры

По мере развития ИКТ все чаще стал обсуждаться вопрос развития виртуальных кластеров (Passiante & Secundo, 2002; Babkin et al., 2013, pp. 68—72; O’Callaghan, 2007, pp. 68—105), то есть таких виртуальных пространств, которые по своим функциям сходны с географическими кластерами, но все взаимодействие происходит онлайн, а участники кластера необязательно находятся в

непосредственной близости друг к другу. Это интересная и по многим параметрам перспективная концепция — она, в частности, позволяет компаниям из малых стран с низким уровнем внутренней конкуренции, находящимся далеко друг от друга, объединяться в такие структуры в виртуальном пространстве для успешной конкуренции на мировом рынке. Однако пока все же по-настоящему успешных виртуальных кластеров не существует. Есть их подобию — профессиональные социальные сети и порталы, но они лишь частично играют роль кластеров. Некоторые эксперты изначально полагали, что в полном смысле создать виртуальные кластеры будет невозможно, так как физическое пространство и живое общение невозможно полностью заменить виртуальными эквивалентами; другие же высказывали мнение, что для некоторых отраслей возникновение таких полноценных виртуальных кластеров возможно, а для некоторых — нет³⁰. Представляется, что второй подход вероятнее, но и в этом случае до формирования полноценных виртуальных кластеров должно еще пройти определенное время.

С течением времени выделились два направления развития виртуальных кластеров. Первое из них представляет собой развитие описанной выше идеи с учетом принципиальных процессов цифровой трансформации, новых технологических возможностей и новых подходов к организации процессов в деловой среде³¹. Вторым — является развитие виртуальных кластеров на основе появления новой системы организации деловых процессов, получившей название «бизнес как платформа». В этом случае кластер формируется на основе деятельности одной компании, которая является системообразующей платформой³². Представляется, что оба подхода к раз-

³⁰ Steele Ch. Industry Clusters Evolving Role in Location Decisions // *Area Development*. Winter 2011. URL: <http://www.areadevelopment.com/siteSelection/jan2011/industry-clusters-evolve-location-decision93090.shtml?Page=1> (accessed: 04.02.2022).

³¹ Про исследования такого направления см., в частности: (Fernández Hurtado et al., 2018).

³² Подробнее об этом см., в частности: (Liping & Zuping, 2019).

витуию виртуальных кластеров равноценны, так как имплементация той или другой модели во многом зависит от отрасли. Вместе с тем следует отметить, что вторая из описанных моделей, как кажется, по состоянию на первый квартал 2022 г. в мире более популярна.

В начале XXI в. израильские исследователи задумались о возможности налаживания инновационного сотрудничества с Палестиной, результатом чего стало их предложение создать виртуальный палестино-израильский инкубатор (Schwartz et al., 2008). Виртуальность появилась, так как в ходе исследования авторы пришли к выводу, что общество с обеих сторон не готово к прямому физическому контакту. Однако вплоть до настоящего времени эта концепция так и не была реализована на практике. Представляется, что одной из причин может быть как раз виртуальность проекта. Здесь есть два объяснения. Во-первых, как отмечалось ранее, виртуальные кластеры (и соответственно инкубаторы) пока еще развиты достаточно слабо, что не позволяет говорить об их эффективности в целом. Во-вторых, уровень общественного развития Ближнего Востока таков, что осуществить переход к сотрудничеству в виртуальном пространстве без фазы сотрудничества в физическом пространстве представляется крайне затруднительным (на самом деле этот тезис верен и для большинства стран Запада).

Вместе с тем из-за пандемии COVID-19, по нашему мнению, произошел принципиальный сдвиг в области цифровой трансформации. Как частные лица, так и компании стали совсем по-другому относиться к возможностям киберпространства. В этой связи возможность виртуализации сотрудничества деловых кругов Израиля и Палестины на основе виртуальной кластеризации не кажется такой уж нереализуемой. Отмеченные нами ранее трансформационные процессы в обеих экономиках позволяют серьезно обсуждать потенциал данного процесса. Такой кластер сегодня вполне способен создать свою финансовую экосистему, что позволит сделать

его наднациональным не только в технологическом смысле.

Нам представляется, что виртуальный кластер может быть своеобразным аналогом особых экономических зон, которые действуют между Израилем и Иорданией (с 1998 г.) и Израилем и Египтом (с 2005 г.). Они являются, по сути, промышленными кластерами, позволяющими участникам получать преференциальный доступ на рынки США, что особенно актуально для израильских партнеров по этим зонам³³.

Виртуализация дает палестинцам возможность избежать длительного и неприятного физического контакта с различными израильскими службами, требующегося при физическом перемещении. При этом палестинцы получают доступ к развитой экономике, которой является Израиль, что расширяет их возможности ведения бизнеса и делового сотрудничества с Израилем в целом (например, работать частным образом и дистанционно в израильских компаниях или оказывать аутсорсинговые услуги как юридическое лицо юридическому лицу).

Платформы взаимодействия

Современная цифровая среда предоставляет представителям израильского и палестинского делового сообществ ряд возможностей по преодолению национальных границ и организации многофакторного сотрудничества по таким направлениям, как: совместная инновационная деятельность, привлечение инвестиций, обучение / менторство. В логике современного уровня развития цифровой экономики обеспечить такую кооперацию может онлайн-платформа, которую в дальнейшем авторы будут называть «платформа взаимодействия» (ПВ).

Такие платформы должны обладать соответствующим функционалом. Так, в первую очередь, ПВ — это возможность свободной коммуникации. Представляется, что существенным элементом ее функционала является организация совместных технологических

³³ Подробнее см., в частности: (Shamel, 2014; Carter et al., 2015).

команд, то есть инноваторы обеих стран могут по определенным протоколам делиться своими идеями с целью формирования совместного бизнеса или привлекать к решению уже существующих задач представителей другой стороны.

Как сама платформа, так и ее пользователи должны иметь возможность привлекать через нее финансовые средства. С учетом всего описанного в предыдущих двух частях работы мы видим довольно перспективным созданием собственной криптовалюты для такой ПВ. Это позволит привлечь к ее деятельности заинтересованных бизнесменов и инвесторов не только из ПНА и Израиля, но и со всего мира, прежде всего — из стран Ближнего Востока и США, включая представителей диаспоры обоих народов. Кроме непосредственно технологических плюсов основным преимуществом такого способа инвестирования в данном случае нам видится его абсолютная политическая и экономическая нейтральность. Любые существующие сегодня платежные средства имеют окраску, так как привязаны к конкретной стране или группе стран, что ввиду застарелого регионального конфликта как у части инвесторов, так и некоторых реципиентов может вызвать нежелательные эмоции. Специально созданная для функционирования ПВ криптовалюта таких эмоций вызывать априори не может.

Следует подчеркнуть, что израильтяне уже сейчас оказывают определенную менторскую поддержку представителям палестинского технологического сообщества, но ее масштаб, как кажется, не соответствует потенциалу формирующейся экосистемы инноваций Палестины. Важным направлением функционирования ПВ должна являться образовательная / менторская деятельность. Специальные онлайн-курсы (предпринимательство, международная инновационная деятельность и проч.), обучающие семинары, сессии бизнес-коучинга — все это способно значительно стимулировать не только развитие инновационной среды в ПНА, но и сблизить палестинцев и израильтян, что позволит им более эффективно сотрудничать.

Ключевым вопросом является вопрос финансирования создания такой ПВ и обеспечения ее функционирования по крайней мере на первом этапе своего существования (в дальнейшем в случае успешного развития ПВ ее функционирование будет оплачиваться как участниками сформированного сообщества, так и за счет работы ряда других инструментов современной экономики, в частности рекламы). Инвесторами в ПВ могут выступить, с одной стороны, такие венчурные фонды, как *Sadara Ventures*³⁴, с другой — институциональные инвесторы из стран Ближнего Востока (в частности ОАЭ), а с третьей — частные инвесторы со всего мира³⁵. Активная цифровизация финансовой системы, в том числе банковской деятельности, проходящая как в Израиле, так и в Палестине (с учетом всех указанных выше проблем), позволит обеспечить соответствующее сопровождение данных процессов.

Трехсторонняя кооперация

Представляется, что воплощение обеих изложенных выше идей палестино-израильского сотрудничества с использованием возможностей цифровой экономики будет крайне затруднено. Однако, во-первых, амбициозные идеи — это как раз двигатель

³⁴ Фонд *Sadara Ventures* создан в 2011 г. американско-израильским предпринимателем и технологическим инвестором Ядином Кауфманом совместно с технологическим предпринимателем из Палестины Саедом Нашефом с целью содействовать развитию современной технологической экономики в ПНА. Фонд является, по сути, первым венчурным фондом, специально созданным для этой цели. По состоянию на середину 2020 г. в его портфеле 6 компаний. Подробнее о фонде см.: *Sadara Ventures*. URL: <https://www.sadaravc.com/> (accessed: 01.09.2021).

³⁵ Нельзя не отметить, что инструмент финансирования развития палестинской экономики, предложенный администрацией экс-президента США Д. Трампа в рамках так называемой «сделки века», может быть как раз одним из существенных источников инвестиций в этот проект. Вместе с тем ввиду того, что возможность реализации данной инициативы крайне низка, в реальности рассчитывать на этот ресурс не представляется возможным. Однако данный документ может быть основой для дальнейших поисков путей разрешения палестино-израильского конфликта, даже принимая во внимание регулярную смену власти в США.

прогресса. Во-вторых, на наш взгляд, существуют механизмы, позволяющие до некоторой степени облегчить их реализацию.

Одним из таких механизмов является привлечение к проекту формирования ПВ третьей стороны. Нам видятся три наиболее вероятных «кандидата» на эту роль: США, Китай и Россия. Прежде чем рассмотреть плюсы и минусы каждого из них, определим-ся с функциями третьей стороны проекта.

На этапе формирования ПВ не исключена вероятность необходимости нейтральной модерации данного процесса (не исключено даже в физическом пространстве), так как стороны могут иметь тенденцию выходить за рамки делового сотрудничества. Наличие нейтрального партнера в данном контексте может оказывать стабилизирующий эффект и при функционировании ПВ.

Несмотря на определенные возможности организации производства (а часть реализуемых через ПВ проектов, безусловно, в итоге предполагает организацию производства) на территории Палестины с учетом наличия дешевой рабочей силы, инфраструктурные ограничения не позволят полностью реализовать имеющийся потенциал сотрудничества. В этой связи возникает необходимость организации производства в другом месте. Безусловно, каждая команда имеет возможность самостоятельно принимать решение о том, где это сделать, но наличие определенного системного предложения, на наш взгляд, позволяет сделать этот процесс более эффективным.

Итак, с точки зрения указанного функционала США выглядят наименее предпочтительным вариантом, так как сегодня они точно совершенно не воспринимаются как нейтральная сторона по отношению к палестино-израильскому конфликту и стоимость организации производства на их территории при всей имеющейся инфраструктуре велика. Однако наличие самой мощной инновационной экономики в мире дает Соединенным Штатам существенное преимущество, так как они могут стать основным источником финансирования ПВ и рынком сбыта результа-

тов инновационной деятельности сформировавшихся на ПВ команд.

Сами США могут быть заинтересованы в таком проекте, так как участие в нем, во-первых, позволяет им реализовывать роль одного из ведущих внешних акторов в регионе Ближнего Востока, используя механизмы «мягкой силы», и, во-вторых, соответствует основным устремлениям, озвученным в экономической части плана Д. Трампа по урегулированию палестино-израильского конфликта³⁶.

Китай, безусловно, интересен и как рынок сбыта, и как производственная площадка. С политической точки зрения он также выглядит достаточно нейтральным. Вместе с тем не исключено, что Китай будет стараться структурировать ПВ таким образом, чтобы извлечь максимальную выгоду именно для себя, без особого учета интересов тех, для кого эта платформа создается.

Китай может быть заинтересован в участии в данном проекте в рамках своей более глобальной стратегии внешнеэкономической экспансии «Пояс и путь» (а также «Нить жемчуга»). В частности, видно, что китайские компании активно работают в израильско-иорданской особой экономической зоне. Однако в описываемом нами случае прямой очевидной мотивации у КНР может не быть.

Российский вариант выглядит интересным, так как сегодня наша страна воспринимается обеими сторонами как нейтральный игрок, в качестве производственной площадки Россия тоже интересна. Однако финансовые возможности Российской Федерации по сравнению с двумя другими потенциальными партнерами являются наиболее скромными.

Сама Россия может быть заинтересована в данном проекте ввиду активного участия Москвы в ближневосточных процессах в целом и стремления сыграть важную роль в решении палестино-израильского конфликта в частности. В данном случае дополнительным стимулом может послужить постоянная необходимость укреплять свои позиции

³⁶ Economic Framework // The White House. URL: <https://trumpwhitehouse.archives.gov/peacetoprospereity/economic/> (accessed: 26.09.2021).

в регионе ввиду соперничества с США за роль лидирующего внешнего игрока.

Существенным недостатком всех трех «кандидатов» является то, что США находятся в настоящий момент в острой фазе соперничества как с Китаем, так и Россией. То есть участие каждой из этих стран в качестве третьего партнера может вызвать серьезную негативную реакцию у другой страны из этого списка и в итоге привести к срыву проекта.

Вместе с тем существует возможность создания представителями делового и политического сообществ указанных стран совместной компании (некоммерческой организации, фонда), которая бы и выступила таким коллективным третьим партнером. Безусловно, такой вариант может выглядеть достаточно утопичным, но ведь инновации — это способ «сказку сделать былью».

Цифровая экономика как инструмент преодоления кризиса

Экономика Палестины практически напрямую зависит от действий Израиля, однако здесь необходимо обратить внимание на следующее. В Палестине достаточно высокий уровень молодых людей с высшим образованием, в том числе девушек, и это число постоянно растет (уровень грамотного населения по состоянию на 2014 г. составлял 98,4 % среди мужчин и 95 % среди женщин)³⁷. Несмотря на небольшие финансовые инвестиции страны в НИОКР и цифровые стартапы, интеллектуальный потенциал Палестины является ее высоколиквидным «человеческим капиталом», так как в настоящее время на смену пребывающей низкоквалифицированной рабочей силы из Палестины на рынок труда могут прийти молодые люди с хорошим потенциалом и багажом знаний в области инноваций. Наряду с этим необходимо отметить заинтересованность не только Израиля, но и богатых арабских стран в недорогой, но высокоинтеллектуальной рабочей силе, что, по нашему мнению, сможет придать

определенный импульс для выхода молодых палестинских специалистов на заинтересованные мировые рынки и обеспечить запуск процессов цифровизации в стране.

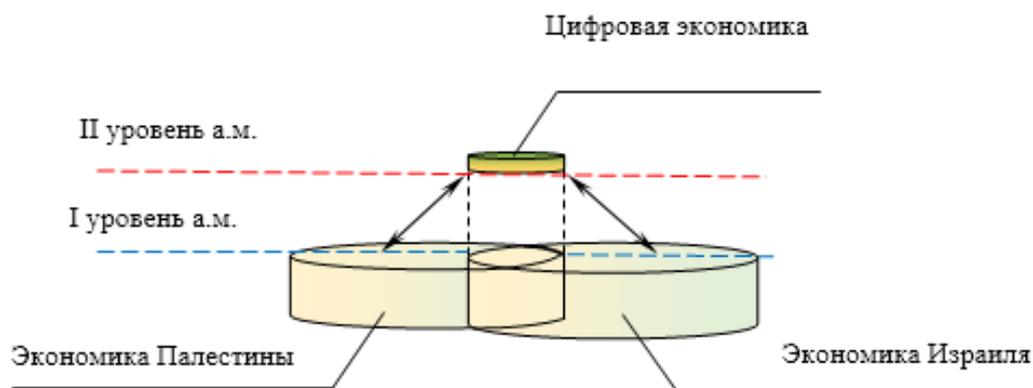
Практика борьбы с пандемией нового коронавируса показала, что у двух стран есть точки соприкосновения перед общей угрозой, так как проводились работы по диагностике выявленных заболевших и штамма вируса, осуществлялся взаимный обмен информацией по всем вопросам, касающимся заболевания и заболевших, на КПП открывались палатки с медицинским оборудованием. Этот факт позволяет надеяться, что и другие социально значимые задачи (а развитие экономики — одна из них) могут решаться в позитивном ключе.

Цифровая экономика предлагает большой спектр возможностей, в том числе в части решения проблем кризиса COVID-19 в долгосрочной перспективе. Конечно, следует оговориться, что в любом случае необходимо принимать пакет антикризисных решений, в частности логистического характера с двух сторон — Палестины и Израиля, а именно: разрешить свободное перемещение товаров, услуг, людей между государствами, а также решить внутренние проблемы самой Палестины, например, провести реформы и прийти к единой концепции по основным вопросам между ФАТХ и ХАМАС.

Цифровая экономика — это шаг вперед. Безусловно, в Израиле она находится на более высоком уровне развития, чем в Палестине, однако, по нашему мнению, именно цифровая экономика и связанные с ней ИКТ являются в нашей терминологии антикризисным *инструментарием II уровня* (рис. 2), который зависит от внутреннего потенциала страны, в том числе человеческого, а также от качества НИОКР, технической оснащенности, при этом он может быть независим от взаимосвязанных элементов, характерных для классического антикризисного инструментария (в настоящей работе авторы назвали его *инструментарием I уровня*, см. рис. 2).

Итак, в целом механизм антикризисного управления представляет собой комплекс методов, при помощи которых осуществляется

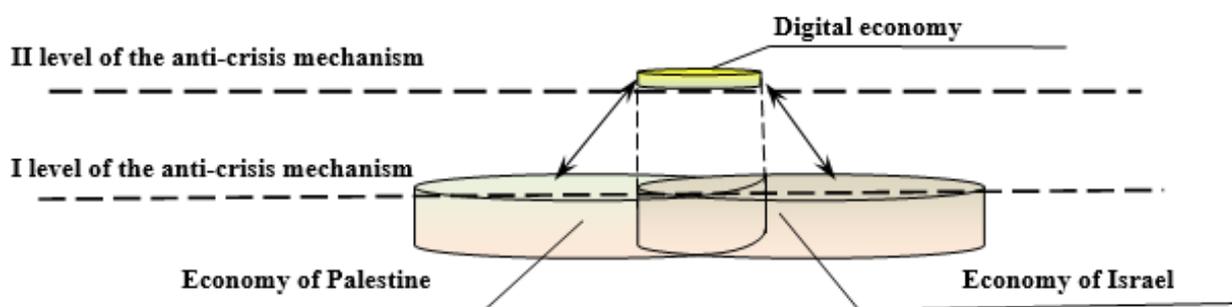
³⁷ Education // The 2014 Palestine Human Development Report. 2014. URL: <https://www.undp.org/content/dam/papp/docs/Publications/UNDP-papp-research-PHDR2015Education.pdf> (accessed: 18.09.2021).



а.м. – антикризисный механизм

↔ – взаимовыгодное сотрудничество

Рис. 2. Цифровая экономика в палестино-израильских отношениях как антикризисный механизм II уровня
 Источник: составлено авторами.



↔ Mutually beneficial cooperation

Fig. 2. The Digital Economy in Palestinian-Israeli Relations as a 2nd Level anti-Crisis Mechanism
 Source: compiled by the authors.

процесс предотвращения кризисов или постепенного выхода из кризисных ситуаций. Эти методы могут включать в себя, например, реструктуризацию долга, продажу активов, вливание дополнительных финансовых средств. Антикризисному управлению посвящены многие книги, учебники и статьи как российских, так и зарубежных авторов, поэтому в данной статье мы не будем подробно останавливаться на основных концепциях этого предмета³⁸. Однако целесообразно

³⁸ См., например: (Балдин и др., 2013; Файншмидт, Юрьева, 2010).

отметить, что включение классического механизма антикризисного управления подразумевает, в первую очередь, проведение ряда необходимых действий, в том числе анализа и оценки финансового состояния субъекта, подготовку плана антикризисных мер, внедрение этих комплексных мер с учетом взвешенного риска. Конечно, будь то банк, предприятие или определенная система в целом (финансовая, социально-экономическая), проведение антикризисных мер требует значительных денежных вливаний, чаще всего из внешних источников, в объект санации. Если рассматривать антикризисные механизмы,

которые могут быть применены к арабским странам, то здесь необходимо отметить в том числе большие денежные переводы от стран-доноров к странам-реципиентам, активное участие в экономической и политической жизни стран различных международных организаций (Всемирный банк, Международный валютный фонд (МВФ)) и т. д.³⁹

Применительно к Палестине следует подчеркнуть следующее: рассмотрев и проанализировав представленные в данном исследовании статистические данные относительно содержания основных статей бюджета, финансового положения страны, его социально-экономической устойчивости, сценарии развития страны (как без последствий COVID-19, так и при наличии глубоко негативных последствий этой пандемии), мы пришли к выводу, что страна находится на грани очень большого кризиса, возможно даже повторения ливанского сценария в части объявления дефолта. Постоянные разногласия между ХАМАС и ФАТХ, необходимые финансовые заимствования органов власти на внутреннем финансовом рынке, разбалансированность в фискальной системе, отсутствие реально работающего промышленного сектора, падение доходов от экспорта и уменьшение инвестиций — все это в полной мере способствует приближению страны к пропасти под названием «дефолт». Ставшая традиционной финансовая помощь в виде траншей от МВФ не может служить той единственной «панацеей» от всех проблем, которые переживает Палестина.

При этом необходимо помнить о существующем уровне зависимости, на которую «подписывается» страна при получении помощи от МВФ и иных «партнерских» организаций: навязывание ими необходимых политических и социальных реформ, полное подчинение руководства страны-заемщика требованиям, выставляемым ему организацией-кредитором. В любом случае, применение классических антикризисных механизмов в решении проблем Палестины, по нашему

мнению, является малоэффективным. В этой связи авторами предложен второй уровень антикризисного механизма (см. рис. 2), под которым понимается антикризисный механизм в рамках цифровой экономики.

Данный уровень не влечет за собой риски, сопряженные с классическим антикризисным механизмом, например, финансовую зависимость от внешних международных организаций. Потенциал этого механизма, в первую очередь, связан с внутренними ресурсами самой страны, грамотным молодым поколением, открытием новых инновационных направлений.

По сути, реализация проектов в рамках базового и начального уровней сотрудничества двух стран в области цифровой экономики как раз и формирует основу антикризисного механизма второго уровня. Логика этого механизма заключается в том, что социально-экономическая активность населения получает возможность реализовываться напрямую — без вмешательства государственных структур обеих стран. Особенно это важно для Палестины. Сферы деятельности с использованием механизмов второго уровня не ограничены только тем, что принято называть инновационной экономикой, ввиду того, что цифровизация потенциально охватывает все сферы национального хозяйства.

Более того, она позволяет гораздо проще находить стороннее финансирование. Коррупционность органов власти Палестины известна. Иностранцы инвесторы, готовые вкладывать средства в развитие территории Палестины, накопили к третьему десятилетию XXI в. усталость от неэффективности расходования этих средств, что вкупе со сложной геополитической обстановкой заставляет их с осторожностью рассматривать такую возможность. Предлагаемые нами цифровые механизмы снимают (по крайней мере, частично) данную проблему.

Применение инструментов цифровой экономики в части механизма антикризисного управления является независимым от мировых экономических потрясений и более гибким при возникновении вызовов на полити-

³⁹ Более подробно см.: (Бабенкова, 2017, с. 9—20).

ческой карте Ближнего Востока. Необходимость в этом инструментарии возрастает, особенно если учесть факт мобилизации палестинской молодежи во время эскалации в 2021 г. между Израилем и Палестиной, включая израильских арабов, которые выступали в том числе за предоставление им равных прав с еврейским населением Израиля.

Заключение

Таким образом, как показано в статье, цифровизация позволяет преодолеть существующие барьеры экономического развития, особенно для Палестины, но главное — она дает возможность деловому сообществу обеих стран существенно снизить значимость текущей неблагоприятной геополитической обстановки и интенсифицировать экономическую составляющую двусторонних отношений. Более того, предлагаемые нами механизмы могут действовать в условиях продолжающегося конфликта, что существенно, так как в таком случае появляется вероятность постепенного улучшения экономической ситуации в Палестине. Это — важная цель сама по себе, так как с экономической точки зрения Израиль значительно более развит и его экономические перспективы существенных вопросов не вызывают.

Несмотря на маловероятную возможность реализации высказанных авторами инициатив в краткосрочной и среднесрочной перспективе, исследование может стать одним из источников позитивных идей при формировании системы эффективного взаимодействия между странами. Ускорение

темпов научно-технического прогресса, обрушившаяся за последние 30 лет на жителей Земли череда изобретений, принципиально изменивших нашу жизнь, сама логика сформулированного одним из провозвестников инновационной экономики Йозефом Шумпетером принципа созидательного разрушения (Schumpeter, 1994, pp. 82—83) позволяют нам сделать вывод, что даже обсуждение сделанных нами предложений является крайне полезным с точки зрения кристаллизации путей дальнейшего развития региона Ближнего Востока в целом.

Дополнительную уверенность в своевременности и необходимости проделанной работы придают авторам происходящие в момент ее написания процессы, а именно — нормализация отношений Израиля и ряда стран арабского мира. Во-первых, сам этот факт показателен — происходит активный процесс деидеологизации палестино-израильского конфликта, что открывает возможность для реализации более прагматичных подходов в организации сосуществования двух народов. Во-вторых, столь кардинальное изменение положения Израиля в регионе (особенно с учетом того, что нормализация уже к моменту написания статьи привела к активному сотрудничеству деловых кругов стран-подписантов) открывает новые возможности для стимулирования развития палестинской экономики, в частности через реализацию намеченных в исследовании направлений двустороннего и многостороннего сотрудничества.

Поступила в редакцию / Received: 03.03.2022
Доработана после рецензирования / Revised: 11.04.2022
Принята к публикации / Accepted: 18.04.2022

Библиографический список

- Ахматшина Э. К., Люкумович Я. Б. «Авраамовы соглашения» между Израилем, ОАЭ и Бахрейном: изменение геополитической реальности Ближнего Востока // *Азия и Африка сегодня*. 2022. № 2. С. 64—68. <https://doi.org/10.31857/S032150750016335-0>
- Бабенкова С. Ю. Ближний Восток: некоторые проблемы антикризисного управления в условиях глобализации // *Ученые записки Российской академии предпринимательства*. Научно-практическое издание. 2017. Т. 16, № 2. С. 9—20.

- Бабенкова С. Ю.* Цифровые финансовые технологии Ближневосточного региона: рассмотрение, анализ, перспективы // *Восточная аналитика*. 2019. № 3. С. 18—30.
- Балдин К. В., Передеряев И. И., Рукоусев А. В.* Антикризисное управление: макро- и микроуровень : учебное пособие. 6-е изд., испр. и доп. Москва : Дашков и К, 2013.
- Коровкин В. В.* Национальные программы цифровой экономики стран Ближнего Востока: опыт сравнения // *Восточная аналитика*. 2019. № 3. С. 53—69.
- Марьясис Д. А.* Экономика и мирное урегулирование на Ближнем Востоке // *Арабо-израильский конфликт: старые проблемы и новые планы* / под ред. А. О. Филоника. Москва : ИБВ, 2003. С. 27—32.
- Морозов В. М., Шебалина Е. О., Лебедева О. В.* Network Diplomacy: Theory // *Электронный научно-образовательный журнал «История»*. 2019. Т. 10, вып. 11 (85). С. 1—3. <https://doi.org/10.18254/S207987840008084-1>
- Новая система производительных сил и страны Востока* / под ред. А. В. Акимова, С. А. Панарина. Москва : ИВ РАН, 2019.
- Перес Ш.* Новый Ближний Восток. Москва : Прогресс, 1994.
- Файнимидт Е. А., Юрьева Т. В.* Зарубежная практика антикризисного управления: учебное пособие. Москва : Евразийский открытый институт, 2010.
- Федорченко А. В., Крылов А. В., Морозов В. М.* Государство Палестина: право на будущее. Москва : МГИМО-Университет, 2018.
- Шваб К.* Четвертая промышленная революция. Москва : Эксмо, 2020.
- Акимова Е. А.* Технологии в обмен на мир: 60-летие агентства по развитию международного сотрудничества (МАШАВ) // *Государство Израиль: путь длиною в 70 лет* / под ред. Т. А. Карасовой, А. В. Федорченко. Москва : МГИМО (У) МИД России, 2019. С. 97—108.
- Babkin A., Kudryavtseva T., Utkina S.* Formation of Industrial Clusters Using Method of Virtual Enterprises // *Procedia Economics and Finance*. 2013. Vol. 5. P. 68—72. [http://doi.org/10.1016/S2212-5671\(13\)00011-7](http://doi.org/10.1016/S2212-5671(13)00011-7)
- Carter A., Gong Y., Nugent J.* Measuring Trade Advantages of the Qualifying Industrial Zones Program of Jordan and Egypt Offered by the United States for Having Signed Peace Treaties with Israel // *Topics in Middle Eastern and North African Economies*. 2015. Vol. 17, no. 2. P. 192—215.
- Cohen H.* Joint Israeli-Palestinian Political Activity in Jerusalem: Characteristics and Challenges // *Locating Urban Conflicts* / ed. by W. Pullan, B. Baillie. London : Palgrave Macmillan, 2013. P. 132—150. https://doi.org/10.1057/9781137316882_8
- Fernández Hurtado S. R., Castillo Triana D., Martínez Martínez L. A.* Clúster virtual: Nueva alternativa a la competitividad eficaz en las empresas // *Tendencias*. 2018. Vol. 19, no. 1. P. 164—186. <https://doi.org/10.22267/rtend.181901.92>
- Liping Z., Zuping Z.* New Development of Traditional Industrial Clusters in China: Virtual Industrial Eco-clusters // *Advances in Social Science, Education and Humanities Research*. Vol. 329: 4th International Conference on Contemporary Education, Social Sciences and Humanities (ICCESSH 2019). Paris : Atlantis Press, 2019. P. 1431—1439. <https://doi.org/10.2991/iccessh-19.2019.317>
- O'Callaghan R.* Towards Dynamic Clustering: Capabilities and IT Enablers // *Digital Business Ecosystems* / ed. by F. Nachira, A. Nicolai, P. Dini, M. Le Louarn, L. R. Leon. Luxembourg : Office for Official Publications of the European Communities, 2007. P. 79—92.
- Passiante G., Secundo G.* From Geographical Innovation Clusters towards Virtual Innovation Clusters: The Innovation Virtual System // *Innovation and New Technologies: 42th European Regional Science Association (ERSA) Congress Report*, 27—31 August 2002. Dortmund : University of Dortmund, 2002. P. 1—22.
- Schroeder Ch.* Startup Rising. The Entrepreneurial Revolution Remaking the Middle East. New York : Palgrave Macmillan, 2013.
- Schumpeter J.* Capitalism, Socialism and Democracy. London : Routledge, 1994.
- Schwartz D., Bar-El R., Malul M.* A Joint Virtual Advanced Technology Incubator — A New Pattern of Israeli-Palestinian Economic Cooperation // *Peace Economics, Peace Science and Public Policy*. 2008. Vol. 14, no. 2. P. 1—17. <https://doi.org/10.2202/1554-8597.1113>
- Seidel T., Abu-Nimer M.* Peace and Reconciliation Processes // *The Wiley Blackwell Encyclopedia of Race, Ethnicity, and Nationalism* / ed. by J. Stone, X. Hou, R. M. Dennis, P. S. Rizova, A. D. Smith. Malden, Mass. : Wiley-Blackwell, 2015. P. 17—19. <https://doi.org/10.1002/9781118663202.wberen148>
- Shamel A.* Trade Regimes and Global Production Networks: The Case of the Qualifying Industrial Zones (QIZs) in Egypt and Jordan // *Geoforum*. 2014. Vol. 57. P. 57—66. <https://doi.org/10.1016/j.geoforum.2014.08.012>

References

- Akhmatshina, E., & Liokumovich, I. (2022). The Abraham accords between Israel, UAE and Bahrain in the context of changing of the geopolitical reality in the Middle East. *Asia and Africa Today*, (2), 64—68. (In Russian). <https://doi.org/10.31857/S032150750016335-0>
- Akimov, A. V., & Panarin, S. A. (Eds.). (2019). *New system of productive forces and Asian countries*. Moscow: IV RAN publ. (In Russian).
- Babenkova, S. Yu. (2017). Middle East: Some problems of anti-crisis management in the context of globalization. *Uchenye Zapiski Rossiiskoi Akademii Predprinimatel'stva. Nauchno-prakticheskoe Izdanie*, 16(2), 9—20. (In Russian).
- Babenkova, S. Yu. (2019). Digital financial technologies of Middle East region: Consideration, analysis, perspectives. *Eastern Analytics*, (3), 18—30. (In Russian).
- Babkin, A., Kudryavtseva, T., & Utkina, S. (2013). Formation of industrial clusters using method of virtual enterprises. *Procedia Economics and Finance*, (5), 68—72. [http://doi.org/10.1016/S2212-5671\(13\)00011-7](http://doi.org/10.1016/S2212-5671(13)00011-7)
- Baldin, K. V., Perederyaev, I. I., & Rukosuev, A. V. (2013). *Anti-crisis management: Macro- and micro-level* : textbook. 6th edition. Moscow: Dashkov and K. publ. (In Russian).
- Carter, A., Gong, Y., & Nugent, J. (2015). Measuring trade advantages of the qualifying industrial zones program of Jordan and Egypt offered by the United States for having signed peace treaties with Israel. *Topics in Middle Eastern and North African Economies*, 17(2), 192—215.
- Cohen, H. (2013). Joint Israeli-Palestinian political activity in Jerusalem: Characteristics and challenges. In W. Pullan & B. Baillie (Eds.), *Locating urban conflicts* (pp. 132—150). London: Palgrave Macmillan. https://doi.org/10.1057/9781137316882_8
- Fainshmidt, E. A., & Yurieva, T. V. (2010). *Foreign practice of anti-crisis management* : textbook. Moscow: Evraziiskii otkrytyi institut publ. (In Russian).
- Fedorchenko, A. V., Krylov, A. V., & Morozov, V. M. (2018). *State of Palestine: A right for the future*. Moscow: MGIMO Universitet publ. (In Russian).
- Fernández Hurtado, S. R., Castillo Triana, D., & Martínez Martínez, L. A. (2018). Clúster virtual: Nueva alternativa a la competitividad eficaz en las empresas. *Tendencias*, 19(1), 164—186. <https://doi.org/10.22267/rtend.181901.92>
- Korovkin, V. V. (2019). National programs of digital economy of the countries of the Middle East: An exercise in comparative analysis. *Eastern Analytics*, (3), 53—69. (In Russian).
- Liping, Z., & Zuping, Z. (2019). New Development of Traditional Industrial Clusters in China: Virtual Industrial Eco-clusters. In *Advances in Social Science, Education and Humanities Research* (Vol. 329; 4th International Conference on Contemporary Education, Social Sciences and Humanities (ICCESSH 2019), pp. 1431—1439). Paris: Atlantis Press. <https://doi.org/10.2991/iccessh-19.2019.317>
- Mariasis, D. A. (2003). Economics and peaceful settlement in the Middle East. In O. Filonik (Ed.), *Arab-Israeli conflict: Old problems and new plans* (pp. 27—32). Moscow: IBV publ. (In Russian).
- Morozov, V., Shebalina, E., & Lebedeva O. (2019). Network Diplomacy: Theory. *Istoriya*, 11(85), 1—3. (In Russian). <https://doi.org/10.18254/S207987840008084-1>
- O'Callaghan, R. (2007). Towards dynamic clustering: Capabilities and IT enablers. In F. Nachira, A. Nicolai, P. Dini, M. Le Louarn & L. R. Leon (Eds.), *Digital business ecosystem* (pp. 79—92). Luxembourg: Office for Official Publications of the European Communities.
- Passiante, G., & Secundo, G. (2002). From geographical innovation clusters towards virtual innovation clusters: The innovation virtual system. In *Innovation and New Technologies, 42th European Regional Science Association (ERSA) Congress Report, 27—31 August 2002* (pp. 1—22). Dortmund: University of Dortmund.
- Peres, Sh. (1994). *The new Middle East*. Moscow: Progress publ. (In Russian).
- Schroeder, Ch. (2013). *Startup rising. The entrepreneurial revolution remaking the Middle East*. New York: Palgrave Macmillan.
- Schumpeter, J. (1994). *Capitalism, socialism and democracy*. London: Routledge.
- Schwab, K. (2020). *The fourth industrial revolution*. Moscow: Eksmo publ. (In Russian).
- Schwartz, D., Bar-El, R., & Malul, M. (2008). A joint virtual advanced technology incubator — a new pattern of Israeli-Palestinian economic cooperation. *The Berkeley Electronic Press*, 14(2), 1—17. <https://doi.org/10.2202/1554-8597.1113>

- Seidel, T., & Abu-Nimer, M. (2015). Peace and reconciliation processes. In J. Stone, X. Hou, R. M. Dennis, P. S. Rizova & A. D. Smith (Eds.), *The Wiley Blackwell encyclopedia of race, ethnicity, and nationalism* (pp. 17—19). Malden, Mass.: Wiley-Blackwell. <https://doi.org/10.1002/9781118663202.wberen148>
- Shamel, A. (2014). Trade regimes and global production networks: The case of the qualifying industrial zones (QIZs) in Egypt and Jordan. *Geoforum*, (57), 57—66. <https://doi.org/10.1016/j.geoforum.2014.08.012>
- Yakimova, E. A. (2019). Technology in exchange for peace: 60th Anniversary of the Agency for the Development of International Cooperation (MASHAV). In T. A. Karasova & A. V. Fedorchenko (Eds.), *The State of Israel: A journey of 70 years* (pp. 97—108). Moscow: MGIMO (U) MID Rossii publ. (In Russian).

Сведения об авторах: *Бабенкова Светлана Юрьевна* — кандидат экономических наук, старший научный сотрудник Центра арабских и исламских исследований Института востоковедения РАН; ORCID: 0000-0001-7369-2720; e-mail: sbabenkova@ivran.ru

Марьясис Дмитрий Александрович — кандидат экономических наук, заведующий Отделом изучения Израиля и еврейских общин Института востоковедения РАН; ORCID: 0000-0002-7910-4552; e-mail: dmaryasis@ivran.ru

Морозов Владимир Михайлович — кандидат исторических наук, доцент кафедры дипломатии МГИМО МИД России; ORCID: 0000-0003-2429-9150; e-mail: morozov@inno.mgimo.ru

About the authors: *Babenkova Svetlana Yuryevna* — PhD (Economics), Senior Research Fellow, Centre of Arabic and Islamic Studies, Institute of Oriental Studies, Russian Academy of Sciences; ORCID: 0000-0001-7369-2720; e-mail: sbabenkova@ivran.ru

Maryasis Dmitry Aleksandrovich — PhD (Economics), Head, Israel and Jewish Communities Studies Department, Institute of Oriental Studies, Russian Academy of Sciences; ORCID: 0000-0002-7910-4552; e-mail: dmaryasis@ivran.ru

Morozov Vladimir Mikhailovich — PhD (History), Associate Professor, Department of Diplomacy, MGIMO-University; ORCID: 0000-0003-2429-9150; e-mail: morozov@inno.mgimo.ru

НАУЧНЫЕ ШКОЛЫ

SCIENTIFIC SCHOOLS

DOI: 10.22363/2313-0660-2022-22-2-342-351

Международная информационная безопасность: в поисках консолидированных подходов

*Интервью с АНДРЕЕМ ВЛАДИМИРОВИЧЕМ КРУТСКИХ,
Специальным представителем Президента Российской Федерации
по вопросам международного сотрудничества в области информационной
безопасности, Чрезвычайным и Полномочным Послом,
директором Департамента международной информационной безопасности
МИД России*

Аннотация. Андрей Владимирович Крутских — Специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности с 2014 г., ведущий эксперт в данной сфере в России и в мире. Он занимал должность председателя Группы правительственных экспертов ООН по достижениям в сфере информации и телекоммуникаций и Группы экспертов государств — членов ШОС по международной информационной безопасности (МИБ). С 2020 г. А.В. Крутских является директором Департамента международной информационной безопасности (ДМИБ) МИД России, с 2017 г. — директором Центра международной информационной безопасности и научно-технологической политики (ЦМИБ) МГИМО МИД России. Андрей Владимирович — автор фундаментальных работ, посвященных вопросам МИБ, научный редактор комплексного учебного пособия «Международная информационная безопасность: теория и практика» (в трех томах), подготовленного авторским коллективом ЦМИБ. В ходе интервью А.В. Крутских рассказал о подходах России в области МИБ, роли Российской Федерации в выработке правил ответственного поведения государств в глобальном информационном пространстве.

Ключевые слова: международная информационная безопасность, информационно-коммуникационные технологии, ООН, РФ, США, КНР



© Крутских А.В., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

Для цитирования: *Крутских А. В.* Международная информационная безопасность: в поисках консолидированных подходов : интервью с Андреем Владимировичем Крутских, Специальным представителем Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности / интервью провел Д. А. Пискунов // *Вестник Российского университета дружбы народов. Серия: Международные отношения.* 2022. Т. 22, № 2. С. 342—351. <https://doi.org/10.22363/2313-0660-2022-22-2-342-351>

International Information Security: In Search of Consolidated Approaches

*Interview with ANDREY V. KRUTSKIKH,
Special Representative of the President of the Russian Federation
for International Cooperation in the Field of Information Security,
Ambassador Extraordinary and Plenipotentiary,
Acting Director of the Department of International Information Security
of the Russian Ministry of Foreign Affairs*

Abstract. Andrey Vladimirovich Krutskikh is the Special Representative of the President of the Russian Federation for International Cooperation in the field of Information Security since 2014, and a leading expert in this field in Russia and around the world. He served as Chairman of the UN Panel of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the SCO Member States Panel of Experts on International Information Security (IIS). Since 2020, A.V. Krutskikh holds the position of Director of the Department for International Information Security (DIIS) of the Ministry of Foreign Affairs of Russia, since 2017 he is Director of the Center for International Information Security, Science and Technology Policy of MGIMO University. Andrey Vladimirovich is the author of fundamental works devoted to IIS issues, the scientific editor of the three volume comprehensive textbook “International Information Security: Theory and Practice,” prepared by the CIIS team of authors. During the interview A.V. Krutskikh spoke about Russia’s approaches to international information security, the role of our country in developing the rules of the responsible State behavior in the global information space.

Key words: international information security, information and communications technologies, United Nations, Russia, United States, China

For citation: Krutskikh, A. V. (2022). International information security: In search of consolidated approaches : Interview with Andrey V. Krutskikh, Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security. Interviewed by D. A. Piskunov. *Vestnik RUDN. International Relations*, 22(2), 342—351. <https://doi.org/10.22363/2313-0660-2022-22-2-342-351>

— Уважаемый Андрей Владимирович, Россия стала инициатором процесса выработки норм, правил и принципов в сфере информационно-коммуникационных технологий (ИКТ) на площадке ООН в 1998 г. Значительные успехи на этом направлении были достигнуты при сотрудничестве с региональными объединениями, такими как СНГ, Организация Договора о коллективной безопасности (ОДКБ), Шанхайская организация сотрудничества (ШОС), БРИКС, Ассоциация государств Юго-Восточной Азии (АСЕАН), Лига арабских государств (ЛАГ),

Африканский союз. Значит ли это, что Россия становится одним из лидеров в области разработки норм в сфере ИКТ?

— Россия стояла у истоков обсуждения проблематики обеспечения международной информационной безопасности (МИБ). В 1998 г. наша страна впервые внесла в Первом комитете Генеральной Ассамблеи ООН проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»¹.

¹ Резолюция ГА ООН A/RES/53/70 «Достижения в сфере информатизации и телекоммуникаций»

Предложенный РФ документ получил поддержку со стороны подавляющего большинства государств — членов Организации.

Профильный переговорный процесс развивался постепенно. В 2001 г. Россия инициировала создание Группы правительственных экспертов ООН (ГПЭ) — узкого по составу формата, в работе которого принимали участие представители 15—25 государств в личном качестве (Бирюков, Алборова, 2019). Цели этого механизма эволюционировали от изучения угроз в ИКТ-сфере до разработки элементов ее регулирования, прежде всего норм, правил и принципов ответственного поведения государств в информационном пространстве. Работа ГПЭ оказалась результативной: в итоговых докладах 2010, 2013 и 2015 гг.², принятых консенсусом, закреплены базовые принципы сотрудничества в области МИБ. В частности, 11 рекомендованных ГПЭ в 2015 г. добровольных правил включены в первоначальный свод международных правил, норм и принципов ответственного поведения государств, закрепленный российской резолюцией Генеральной Ассамблеи ООН № 73/27³.

в контексте международной безопасности» // ООН. 04.01.1999. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R (дата обращения: 01.04.2022).

² См.: Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2010 г. (A/65/201) // ООН. 30.07.2010. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/65/201&referer=/english/&Lang=R (дата обращения: 01.04.2022); Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2013 г. (A/68/98) // ООН. 24.06.2013. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R (дата обращения: 01.04.2022); Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2015 г. // ООН. 22.07.2015. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement> (дата обращения: 01.04.2022).

³ Резолюция ГА ООН A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // ООН. 11.12.2018. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/07/PDF/N1841807.pdf?OpenElement> (дата обращения: 01.04.2022).

С течением времени круг государств, желающих участвовать и иметь право голоса в ооновской дискуссии по МИБ, расширялся. В ответ на запрос международного сообщества в 2018 г. Россия предложила создать качественно новый переговорный механизм — Рабочую группу ООН открытого состава (РГОС). Ее принципиальное отличие от ГПЭ — возможность всех без исключения государств — членов ООН «на равных» участвовать в процессе принятия конкретных решений в области МИБ и отстаивать интересы национальной безопасности. РГОС, известная как «Кибер-Генассамблея», является первым универсальным, инклюзивным, прозрачным и подлинно демократичным переговорным механизмом по проблематике МИБ в системе ООН (Зиновьева, 2020). Несмотря на трудности, обусловленные пандемией, РГОС успешно завершила свою деятельность в марте 2021 г. принятием итогового доклада консенсусом всех 193 государств — членов ООН⁴.

31 декабря 2020 г. по инициативе России при поддержке внушительного большинства государств Генеральная Ассамблея ООН в ходе своей 75-й сессии одобрила российский проект резолюции, постановляющий созвать начиная с 2021 г. новую РГОС по вопросам безопасности в сфере использования ИКТ и самих ИКТ на период 2021—2025 гг.⁵ Такое решение служит подтверждением актуальности и необходимости обеспечения глобального переговорного процесса по вопросам МИБ. Следует отметить, что новая РГОС уполномочена обсуждать выдвигаемые государствами профильные предложения, вопросы наращивания потенциала, а также налаживания диалога стран (при их лидирующей роли) с

⁴ Доклад Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2021 г. // ООН. 18.03.2021. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/068/74/PDF/N2106874.pdf?OpenElement> (дата обращения: 01.04.2022).

⁵ Резолюция Генеральной Ассамблеи ООН A/RES/75/240 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // ООН. 04.01.2021. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf?OpenElement> (дата обращения: 01.04.2022).

бизнесом, неправительственными организациями и научно-академическим сообществом.

Успех Группы зависит от целой серии факторов, среди которых ключевой — ее субстантивное наполнение. Принципиально важно придать деятельности РГОС максимально прагматичный и практико-ориентированный характер, чтобы итогом ее работы стали прикладные нормы, рекомендации и программы помощи.

Безусловно, значительные успехи на этом направлении достигнуты при сотрудничестве с региональными объединениями. Россия активно взаимодействует с государствами СНГ, ОДКБ, ШОС, БРИКС, АСЕАН, Региональный форум АСЕАН (АРФ), ЛАГ, Африканского союза. Работа на данных площадках направлена на согласование конкретных решений по обеспечению МИБ. Выработка норм, правил и принципов ответственного поведения активно обсуждается в БРИКС и ШОС. Противодействие информационной преступности — один из ключевых аспектов дискуссии по линии ОДКБ, СНГ, АСЕАН, АРФ. В рамках АСЕАН идет разработка понятийного аппарата в сфере безопасного использования ИКТ. Россия также заключила целый ряд двусторонних межправительственных соглашений, которые позволяют углублять диалог с государствами-единомышленниками в сфере МИБ (Крутских, Бирюков, 2017).

Можно сказать, что Россия продолжает задавать тон международному сотрудничеству в данной области, добиваясь выработки правил ответственного поведения под эгидой ООН, которые должны базироваться на следующих принципах:

- суверенное равенство;
- разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир, безопасность и справедливость;
- отказ от применения силы или угрозы силой как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями ООН;
- уважение прав человека и основных свобод;

– невмешательство во внутренние дела других государств⁶.

— Какие школы осмысления обеспечения МИБ, на ваш взгляд, сложились на сегодняшний день в мире? Какие исследовательские инициативы, а также каких авторитетных экспертов вы можете отметить в этой связи? Можно ли разделить их на группы в зависимости от подходов?

— В настоящее время важную роль в международном сотрудничестве играет публичная дипломатия. К обсуждению различных аспектов МИБ активно подключаются представители научно-академического сообщества. На базе МГИМО МИД России функционирует Центр международной информационной безопасности и научно-технологической политики (ЦМИБ), который непосредственно вовлечен в обсуждение вопросов использования ИКТ в рамках РГОС, а также на региональных и двусторонних площадках⁷. В марте 2022 г. сотрудники ЦМИБ приняли участие в неформальной онлайн-встрече председателя РГОС Б. Гафура с представителями заинтересованных негосударственных сторон, после чего был опубликован аналитический доклад ЦМИБ об основных подходах России по МИБ (*International Information Security...*, 2021). Помимо этого, сотрудники Центра на регулярной основе выступают на мероприятиях по линии СНГ, ОДКБ, ШОС, БРИКС, АРФ и АСЕАН.

ЦМИБ вносит важный вклад в подготовку профессиональных кадров. В 2019 г. был выпущен учебник в трех томах «Международная информационная безопасность: теория и практика» (2019), который в 2021 г. был переиздан и дополнен (Международная информационная безопасность: теория и практика,

⁶ Резолюция Генеральной Ассамблеи ООН A/RES/75/240 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // ООН. 04.01.2021. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf?OpenElement> (дата обращения: 01.04.2022).

⁷ Центр международной информационной безопасности и научно-технологической политики // МГИМО МИД России. URL: <https://mgimo.ru/about/structure/ucheb-nauch/ciis/> (дата обращения: 01.04.2022).

2021). Это первое в мире комплексное издание по данной теме, представляющее собой фактически научную онтологию по МИБ. На базе учебника был подготовлен инновационный цифровой образовательный комплекс «Международная информационная безопасность: теория и практика», который был выдвинут на премию Правительства России в области образования за 2021 г. и вошел в «короткий список» номинантов.

В рамках программы «Приоритет — 2030» ЦМИБ подготовил доклад «Международная информационная безопасность: подходы России», в котором в доступном для широкой аудитории формате представлены самые насущные проблемы МИБ, а также комплексно охарактеризованы подходы России к формированию международного режима в области безопасности ИКТ на глобальном, региональном и двустороннем уровнях (International Information Security: Russia's Approaches, 2021). Доклад был представлен на площадке ООН и получил широкое признание в академическом и дипломатическом сообществе.

Кроме того, на площадке МГИМО проходят конференции, форумы, семинары и круглые столы, в ходе которых обсуждаются актуальные аспекты цифровой повестки дня с учетом перспективных направлений технологического развития и современных трансформаций международной системы. Подобный обмен мнениями способствует формированию комплексного представления о перспективных направлениях внутренней политики и взаимодействия на международном уровне в данной области.

Можно сказать, что вокруг ЦМИБ сформировалась уникальная научная школа МГИМО в области исследования международной информационной безопасности и научно-технологической политики. Центр отстаивает национальные интересы Российской Федерации и оказывает экспертную поддержку экспертам страны в данной сфере. Научные труды ЦМИБ широко цитируются российскими и зарубежными учеными и задают направление для дальнейшей проработки этих вопросов и подготовки нового поколения исследователей. Сотрудники Центра

активно публикуют статьи в научных изданиях, за их авторством выходят монографии, учебная и методическая литература.

Практико-ориентированное направление научных исследований в области МИБ формируется на базе созданной в 2018 г. Национальной Ассоциации международной информационной безопасности (НАМИБ)⁸. Президентом Ассоциации является советник секретаря Совета Безопасности РФ В.П. Шерстюк, члены Ассоциации — ведущие эксперты страны в области МИБ. Наблюдательный совет НАМИБ возглавляет заместитель секретаря Совета Безопасности РФ О.В. Храмов. Согласно Уставу Ассоциации, одной из основных ее целей является содействие продвижению российских инициатив в области обеспечения МИБ с проработкой в упреждающем режиме проблемных вопросов в интересах формирования переговорных позиций государственных органов. При обсуждении проекта «Основ государственной политики Российской Федерации в области международной информационной безопасности» 26 марта 2021 г. президент России В.В. Путин особо подчеркнул роль НАМИБ в реализации государственной политики России на данном направлении⁹.

Действительно, в условиях, когда коллективный Запад развязал против России агрессивную кибервойну, взаимодействие по линии научно-академического сообщества имеет особое значение, поскольку многие контакты с Россией на государственном уровне по обеспечению МИБ прерваны. Углубленный экспертный разговор на полуторном треке — уникальный источник идейной «подпитки» усилий России на международной арене и в то же время объективного и нетривиального взгляда на перспективы многосторонней дискуссии.

⁸ Национальная Ассоциация Международной Информационной Безопасности (НАМИБ). URL: <https://namib.online/> (дата обращения: 01.04.2022).

⁹ Президент провел в режиме видеоконференции заседание Совета Безопасности, в ходе которого рассматривался проект «Основ государственной политики Российской Федерации в области международной информационной безопасности» // Совет Безопасности РФ. 26.03.2021. URL: <http://www.scrf.gov.ru/news/speeches/2952/> (дата обращения: 01.04.2022).

НАМИБ, в свою очередь, обладает богатым опытом проведения международных форумов и конференций, в том числе в Гватемале, Германии, Китае, на Кубе и т. д. В условиях пандемии Ассоциацией организован форум «Партнерство государства, бизнеса и гражданского общества при обеспечении МИБ», выпущены сборники докладов, а также аналитические, научные и методические работы¹⁰.

Молодые исследователи также вовлекаются в научное осмысление МИБ и переговорную деятельность на данном направлении. Локомотивом для продвижения молодежных инициатив служит Школа международной информационной безопасности Дипломатической академии МИД России, которая регулярно проводит на своей площадке открытые лекции по актуальным аспектам МИБ, участвует в научных конференциях, семинарах и круглых столах по профильной тематике¹¹.

Проблематика обеспечения МИБ интересует и зарубежных исследователей. Нельзя не отметить ведущие научные центры КНР, которые занимаются изучением данного направления и прикладной работой. Прежде всего, речь идет об Ассоциации Интернета Китая¹², Китайской ассоциации безопасности киберпространства¹³, Комитете федерации промышленности и торговли по эксплуатации и обслуживанию больших данных¹⁴, Центре

безопасности «360»¹⁵. Значительное внимание китайское научно-академическое сообщество уделяет изучению глобального управления Интернетом. Янь Сюэтуан, директор Института современных международных отношений Университета Цинхуа, главный редактор «Китайского журнала о международной политике», рассматривает киберпространство в качестве ключевого драйвера развития мировой политики и международных отношений. Он выделяет глобальное управление киберпространством в качестве стратегической области противостояния США и КНР (Yan Xuetong, 2020). Кроме того, особое место в литературе КНР занимает проблематика технологической конкуренции США и КНР и ее последствий для глобального управления Интернетом (Li Zhi & Tang Runhua, 2020). Ряд авторов рассматривают китайский подход к глобальному управлению Интернетом в контексте национальной безопасности и цифрового суверенитета (Xu Peixi, 2021; Wang Zheng, 2020).

Исследованием проблематики кибербезопасности и роли КНР в ее обеспечении занимается Лаборатория Лейденского университета под руководством Р. Кримерса в рамках проекта *China's Role in Cyber Security*¹⁶. Р. Кримерс, профессор Лейденского университета, соучредитель проекта *DigiChina*, исследует регулирование КНР в области цифровых технологий, а также политику Китая в глобальном управлении Интернетом (Creemers, 2022).

Двусторонние отношения России и Китая носят характер всеобъемлющего стратегического партнерства. Наши страны придерживаются схожих взглядов в области обеспечения МИБ, поддерживают выработку под эгидой ООН правил ответственного поведения государств в информпространстве.

Подходы западных стран отличаются от продвигаемых Россией и Китаем. Главным достижением научной школы коллективного

¹⁰ Программа XV международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении МИБ» // НАМИБ. 24.09.2021. URL: <https://namib.online/2021/09/programma-xvmezhdunarodnogo-foruma-partnerstvo-gosudarstva-biznesa-i-grazhdanskogo-obshhestva-pri-obespechenii-mezhdunarodnoj-informacionnoj-bezopasnosti/> (дата обращения: 01.04.2022).

¹¹ Школа МИБ // Дипломатическая академия МИД России. URL: <https://www.dipacademy.ru/special-projects/mib-school/> (дата обращения: 01.04.2022).

¹² Zhongguo hulianwang xiehui [Интернет-сообщество Китая]. URL: <https://www.isc.org.cn> (accessed: 01.04.2022). (На китайском языке).

¹³ Zhongguo wangluo kongjian anquan xiehui [Ассоциация кибербезопасности Китая]. URL: <https://www.cybersac.cn> (accessed: 01.04.2022). (На китайском языке).

¹⁴ Zhonghua quanguo gongshangye lianhehui [Всекитайская федерация промышленности и торговли]. URL: https://www.acfic.org.cn/zjzg_327/zmwyh/2021_wlaqwylh/2021_wlaqwylh_md (accessed: 01.04.2022). (На китайском языке).

¹⁵ 360 qiye anquan hui [Ассоциация корпоративной безопасности «360»]. URL: <https://www.360.cn> (accessed: 01.04.2022). (На китайском языке).

¹⁶ *China's Role in Cyber Security* // Leiden Asia Centre. URL: <https://leidenasiacentre.nl/chinas-role-in-cyber-security/> (accessed: 01.04.2022).

Запада в области МИБ (следует отметить, что в западном научном дискурсе чаще используется термин «кибербезопасность») считается публикация Таллиннского руководства и Таллиннского руководства 2.0 о применимости международного права к конфликтам и войнам в информационной сфере, подготовленного сотрудниками Центра киберзащиты НАТО в Таллинне под руководством профессора права М. Шмидта¹⁷. Данное издание — академический научный труд, не имеющий обязательной юридической силы, но претендующий на продвижение западной переговорной позиции по МИБ, по сути допускающей использование ИКТ в военных целях. Следует также отметить, что внутри западной научной школы в данной области имеют место существенные содержательные и идеологические расколы.

В этом контексте хотелось бы отметить, что Россия выступает за более активное вовлечение бизнеса, неправительственных организаций и научно-академического сообщества в глобальную дискуссию по вопросам обеспечения информбезопасности. На наш взгляд, специфика ИКТ такова, что представители негосударственных субъектов могут внести весомый содержательный вклад в решение задач, стоящих перед международным сообществом.

— В 2020 г. китайские компании China Mobile и Huawei при поддержке заинтересованных министерств выдвинули предложение в рабочей группе МСЭ о разработке новых протоколов IP-адресов, способствующих дальнейшему развитию передовых технологий, в том числе 5G. Как вы считаете, могут ли предложенные стандарты стать альтернативой существующим протоколам сети Интернет, созданным по запросам Запада?

¹⁷ Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence / ed. by M.N. Schmitt. Cambridge; New York : Cambridge University Press, 2013. URL: https://assets.cambridge.org/97811070/24434/frontmatter/9781107024434_frontmatter.pdf (accessed: 01.04.2022).

— Ключевую роль в управлении Сетью играют Корпорация по управлению доменными именами и IP-адресами (ICANN)¹⁸ и ее дочерняя структура — Организация по открытым техническим идентификаторам (PTI)¹⁹. Несмотря на то, что ICANN формально является независимой некоммерческой организацией, фактически контроль над распределением имен и адресов Интернета осуществляет правительство США. Негосударственный статус ICANN выступает в роли «ширмы», призванной прикрыть американскую гегемонию США.

Что касается Международного союза электросвязи (МСЭ)²⁰, то данная специализированная структура ООН ни юридически, ни политически не вовлечена в управление Интернетом, поскольку ее участие в данном процессе открыто саботируют США и их партнеры. Россия уже давно выступает за передачу прерогатив по управлению Интернетом МСЭ, который обладает необходимой экспертизой и легитимностью в данных вопросах (Зиновьева, 2009). Естественно, такие предложения противоречат принципиальным подходам США по сохранению контроля над Сетью.

Россия и Китай последовательно выступают за интернационализацию управления глобальной сетью Интернет, повышение роли государств в этом процессе, а также сохранение их суверенного права регулировать национальный сегмент Интернета (International Information Security..., 2021). Китай также активно участвует в принятии универсальных стандартов в области сетей связи пятого поколения 5G. Со стороны Китая и китайских компаний ведется работа по разработке новых протоколов IP-адресов. Все эти действия в конечном итоге направлены на интернационализацию международного управления Интернетом и повышение роли глобального сообщества в данном процессе в целях

¹⁸ The Internet Corporation for Assigned Names and Numbers (ICANN). URL: <https://www.icann.org/en> (accessed: 01.04.2022).

¹⁹ Public Technical Identifiers (PTI). URL: <https://pti.icann.org/> (accessed: 01.04.2022).

²⁰ International Telecommunication Union. URL: <https://www.itu.int/ru/Pages/default.aspx> (accessed: 01.04.2022).

придать ему инклюзивный и демократичный характер (Routledge Handbook of International Cybersecurity, 2020). Повторю, оптимальной институциональной базой для этого является МСЭ.

— США заморозили сотрудничество с Россией по вопросам кибербезопасности. Страны Запада на сессии Рабочей группы ООН открытого состава обвинили Россию во вредоносной деятельности в информационном пространстве. Как дальше будет развиваться диалог между Россией и Западом в многостороннем и двустороннем форматах по выработке конвенции об обеспечении МИБ?

— Россия и США — страны, которые несут особую ответственность за поддержание глобального мира и безопасности. Наше взаимодействие выстраивалось по-разному, но с неизменным настроем России на достижение практических результатов.

25 сентября 2020 г. президент Российской Федерации В.В. Путин выступил с комплексной программой практических мер по восстановлению российско-американского сотрудничества в области МИБ²¹. Программа была ориентирована на повышение уровня доверия, перезагрузку отношений с США в целях недопущения масштабной конфронтации в цифровой среде и включала в себя следующие направления:

1) восстановление полномасштабного двустороннего регулярного межведомственного диалога по ключевым вопросам обеспечения МИБ на высоком уровне;

2) поддержание непрерывной и эффективной работы каналов связи между компетентными ведомствами наших стран по линии Центров по уменьшению ядерной опасности, Групп оперативного реагирования на компьютерные инциденты и должностных лиц высокого уровня, курирующих эту проблематику в рамках структур, связанных с вопросами

обеспечения национальной, в том числе информационной, безопасности;

3) совместная разработка и заключение двустороннего межправительственного соглашения о предотвращении инцидентов в информационном пространстве по аналогии с действующим советско-американским Соглашением о предотвращении инцидентов в открытом море и воздушном пространстве над ним от 25 мая 1972 г.;

4) обмен во взаимоприемлемой форме гарантиями невмешательства во внутренние дела друг друга, включая избирательные процессы, в том числе с использованием ИКТ и других высокотехнологических методов.

Кроме того, президентом Российской Федерации В.В. Путиным было предложено выйти на заключение глобальной договоренности о принятии государствами политического обязательства о ненанесении первыми удара с использованием ИКТ. Предметной реакции на российское предложение не последовало.

После июльского саммита в 2021 г. в Женеве между Россией и США был запущен профильный экспертный диалог в формате «Кремль — Белый дом» под эгидой аппарата Совета Безопасности Российской Федерации и Совета национальной безопасности США²². Был налажен обмен оперативной информацией по киберпреступлениям, увеличен объем и качество информации о компьютерных инцидентах, передаваемой между Национальным координационным центром по компьютерным инцидентам России и Агентством кибербезопасности и защиты инфраструктуры США. Активизировалось двустороннее взаимодействие Генеральной прокуратуры Российской Федерации с Министерством юстиции США. Тем не менее, несмотря на опыт позитивного взаимодействия в данной сфере, весной 2022 г. Белый дом в одностороннем порядке вышел из единственного постоянно действующего канала связи с Кремлем. Кроме того, Вашингтон отказался от дальнейшего обсуждения вопросов безопасности

²¹ Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности // Президент России. 25.09.2020. URL: <http://kremlin.ru/events/president/news/64086> (дата обращения: 01.04.2022).

²² Белый дом и Кремль согласились, что диалог — лучший способ деэскалации // Интерфакс. 31.12.2021. URL: <https://www.interfax.ru/world/813561> (дата обращения: 01.04.2022).

объектов критической информационной инфраструктуры. Была остановлена и вся совместная работа по пресечению деятельности киберпреступников. США отказались от российского предложения деанонимизировать Интернет и принудили своих союзников не поддерживать нашу инициативу о принятии международного юридически обязывающего документа, регулирующего деятельность государств в информпространстве.

Вследствие односторонней и деструктивной позиции коллективного Запада снижается общий уровень информационной безопасности в мире. Количество кибератак последние годы растет. С начала 2022 г. западные страны многократно нарастили атаки на нашу страну — до миллиона в неделю.

20 мая 2022 г. под председательством президента Российской Федерации В.В. Путина состоялось заседание Совета Безопасности Российской Федерации, в ходе которого обсуждались вопросы информационной безопасности²³. Президент России отметил, что в настоящее время предпринимаются целенаправленные попытки вывести из строя интернет-ресурсы объектов критической информационной инфраструктуры России²⁴. В первую очередь под ударом оказались средства массовой информации, финансовые учреждения, социально значимые порталы. Кроме того, инструментом санкционного давления на Россию со стороны Запада стали ограничения на зарубежные информационные технологии, программы и продукты. Многие западные поставщики в одностороннем порядке прекратили техническую поддержку своего оборудования в России. Участились случаи ограничения работы или даже блокировки программ после их обновления. Однако уже сегодня можно сказать, что киберагрессия против России, как и в целом санкционный наскок на нашу страну, провалилась. В целом мы были готовы к этой атаке, и это

²³ Под председательством Владимира Путина в режиме видеоконференции состоялось заседание Совета Безопасности Российской Федерации // Совет Безопасности РФ. 20.05.2022. URL: <http://www.scrf.gov.ru/news/allnews/3240/> (дата обращения: 21.05.2022).

²⁴ Там же.

результат той системной работы, которая велась все последние годы²⁵.

Вне зависимости от геополитической обстановки Россия остается открытой к диалогу и сотрудничеству на принципах взаимного доверия и уважения национальных интересов со всеми государствами, и США в этом смысле не исключение.

Что касается Конвенции об обеспечении МИБ, то впервые идея была озвучена Российской Федерацией в Екатеринбурге в 2011 г. на встрече высоких представителей, курирующих вопросы безопасности. Соавторами российского проекта тогда выступили 52 государства²⁶. Обновленный проект Конвенции Россия представила в 2021 г. Сегодня ключевой площадкой для обсуждения положений будущей Конвенции об обеспечении МИБ является РГОС. В целях поддержания стратегической стабильности и обеспечения защиты от киберугроз недостаточно норм, которые носят добровольный и рекомендательный характер, требуется юридическое закрепление «правил дорожного движения» в ИКТ-среде.

— Как вы считаете, ускорится ли в перспективе процесс технологического разъединения на Запад, придерживающийся своей парадигмы кибербезопасности, и не-Запад, отстаивающий концепцию международной информационной безопасности и суверенное управление внутренним сегментом сети Интернет?

— Тенденции последних лет и тем более месяцев свидетельствуют о том, что раскол мирового сообщества на Запад и не-Запад продолжается.

Цель США и стран НАТО — восстановить и навеки закрепить свое доминирование в международных делах, чтобы решать собственные узкокорыстные задачи в ущерб национальным интересам других членов международного сообщества. Они противопоставляют пресловутый «миропорядок,

²⁵ Заседание Совета Безопасности // Президент России. 20.05.2022. URL: <http://kremlin.ru/events/president/news/68451> (дата обращения: 21.05.2022).

²⁶ Россия указала выход для интернета // Коммерсантъ. 23.09.2011. URL: <https://www.kommersant.ru/doc/1779208> (дата обращения: 01.04.2022).

основанный на правилах», который на практике означает закрепление права сильного в мировых делах, традиционному пониманию системы международных отношений, основанной на международном праве.

Россия и ее единомышленники выступают за развитие всеобъемлющего сотрудничества в области МИБ с учетом интересов всех государств. Первостепенная задача — выработка международно-правовых основ деятельности стран, а также неправительственных субъектов в сфере ИКТ.

Текущая обстановка на глобальной арене едва ли располагает к оптимистическим прогнозам. Тем не менее безопасность в киберсфере требует международных договоренностей. Ставки слишком высоки, чтобы полагаться на игру без правил.

Невозможно существование кибермира, в котором отдельные государства стремятся

укрепить свою безопасность за счет безопасности других. Необходимо всем мировым сообществом работать над предотвращением конфликтов в информационном пространстве, продвижением мирного использования ИКТ, недопущением их применения в преступных и террористических целях, а также продолжением профильных переговоров при центральной роли ООН. Иначе, как заявил С.В. Лавров, миру грозит киберанархия²⁷.

²⁷ Выступление Министра иностранных дел Российской Федерации С.В. Лаврова на пленарной сессии «Международные отношения в условиях цифровизации общественной жизни» международной научно-практической конференции «Цифровые международные отношения 2022», Москва, 14 апреля 2022 года // МИД России. 14.04.2022. URL: https://www.mid.ru/ru/foreign_policy/news/1809294/ (дата обращения: 01.05.2022).

Интервью провел Д.А. Пискунов / Interviewed by D.A. Piskunov

Поступила в редакцию / Received: 10.05.2022

Библиографический список

- Бирюков А. В., Алборова М. Б. Социально-гуманитарное измерение международной информационной безопасности. Москва : Аспект Пресс, 2019.
- Зиновьева Е. С. Международная информационная безопасность: проблемы многостороннего и двустороннего сотрудничества. Москва : МГИМО, 2020.
- Зиновьева Е. С. Международное управление интернетом: конфликт и сотрудничество. Москва : МГИМО, 2009.
- Крутских А., Бирюков А. Новая геополитика международных научно-технологических отношений // *Международные процессы*. 2017. № 2. С. 6—26.
- Международная информационная безопасность: теория и практика* : в 3 т. / под общ. ред. А. В. Крутских. Москва : Аспект Пресс, 2019.
- Международная информационная безопасность: теория и практика* : в 3 т. / под общ. ред. А. В. Крутских. Москва : Аспект Пресс, 2021.
- Creemers R. China's Cybersecurity Regime: Securing the Smart State. Leiden University, 2022. P. 1—38. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4070682 (accessed: 01.04.2022).
- International Information Security: Russia's Approaches* / ed. by A. Krutskikh, E. Zinovieva. Moscow, 2021.
- Li Zhi, Tang Runhua. Duo li yi you guan fang mo shi : gou jian quan qiu hu lian wang zhi li ti xi de lu jing yan jiu [Многосторонняя модель: путь к созданию глобальной системы управления Интернетом] // *Chuan mei guan cha* [Медиа обозреватель]. 2020. Vol. 444, no. 12. P. 21—28. (На китайском языке).
- Routledge Handbook of International Cybersecurity* / ed. by E. Tikk, M. Kerttunen. Routledge, 2020.
- Wang Zheng. Lian he guo "shuang gui zhi" xia quan qiu wang lu kong jian gui ze zhi ding xin tai shi [Глобальное управление Интернетом на пути к цифровой холодной войне или цифровому достоянию] // *Zhong guo xin xi an quan* [Информационная безопасность Китая]. 2020. Vol. 20, no. 1. P. 40—43. (На китайском языке).
- Xu Peixi. 2020 shu zi leng zhan yuan nian: wang lu kong jian quan qiu zhi li de liang zhong lu xian zhi zheng [Год цифровой холодной войны 2020: битва двух путей глобального управления в киберпространстве] // *Xin xi an quan yu tong xin bao mi* [Информационная безопасность и конфиденциальность связи]. 2021. Vol. 21, no. 3. P. 16—23. (На китайском языке).
- Yan Xuetong. Bipolar Rivalry in the Early Digital Age // *The Chinese Journal of International Politics*. 2020. Vol. 13, no. 3. P. 313—341. <https://doi.org/10.1093/cjip/poaa007>



ПРИКЛАДНОЙ АНАЛИЗ

APPLIED ANALYSIS

DOI: 10.22363/2313-0660-2022-22-2-352-371

Научная статья / Research article

Ценностный суверенитет в эпоху глобальных конвергентных медиа

Д.А. Дегтерев  

Российский университет дружбы народов, Москва, Российская Федерация
МГИМО МИД России, Москва, Российская Федерация
СПбГУ, Санкт-Петербург, Российская Федерация
 degterev-da@rudn.ru

Аннотация. Суверенитет в цифровом пространстве — это относительно новый, сравнительно малоизученный феномен, который рассматривается в данной статье. Он носит комплексный характер и зависит как от используемой технологической базы (прежде всего, сетевого оборудования, в том числе 5G и др.), программных продуктов и платформ, так и от продвигаемого контента. Перед странами встает непростая задача регулирования деятельности глобальных медиахолдингов для сохранения ценностного суверенитета. Автор приводит политэкономический анализ ценностного суверенитета, показывая важность государства как регулятора, позволяющего устранять негативные информационные экстерналии. Особое внимание уделяется анализу международного медиапейзажа и формированию многополярности в сетевом пространстве, в том числе усиливающемуся феномену технологической конвергенции в медиаиндустрии, а также позициям отдельных стран и регионов в глобальной медиаиндустрии. Рассматриваются корпоративные структуры крупнейших медиахолдингов мира, и выявляется усиливающаяся степень диверсификации их активов. Исследуются поколенческая дифференциация механизмов социализации в постпандемную эпоху, в том числе доля времени, уделяемого социальным платформам, традиционным СМИ (на примере телевидения), а также основные способы доступа в Интернет и проникновения новых технологий. Показаны наиболее перспективные для социализации и быстрорастущие сегменты, в частности интернет-телевидение, технологии создания виртуальной реальности, видеоигры и киберспорт. В финальной части статьи рассматриваются основные проблемы и вызовы регулированию национального медиапространства с целью обеспечения ценностного суверенитета в эпоху глобальных конвергентных медиа.

Ключевые слова: ценности, суверенитет, политэкономия, информационные экстерналии, социальные платформы, медиа, конвергенция, государственное регулирование

Благодарности: Исследование выполнено в рамках исследовательского проекта РФФИ-ЭИСИ № 21-011-31812 на тему «Имитационное моделирование распространения социальных норм и ценностей: глобальные коммуникации VS информационный суверенитет РФ».

© Дегтерев Д.А., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

Для цитирования: Дегтерев Д. А. Ценностный суверенитет в эпоху глобальных конвергентных медиа // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 352—371. <https://doi.org/10.22363/2313-0660-2022-22-2-352-371>

Value Sovereignty in the Era of Global Convergent Media

Denis A. Degterev  

Peoples' Friendship University of Russia (RUDN University), Moscow, Russian Federation
MGIMO University, Moscow, Russian Federation
Saint-Petersburg State University, Saint-Petersburg, Russian Federation
 degterev-da@rudn.ru

Abstract. Sovereignty in the digital space is a relatively new phenomenon, which is discussed in this paper. It is complex in nature and depends both on the technological base which is used (primarily network equipment, including 5G, etc.), software products and platforms, and on the promoted content. The countries are faced with the difficult task of regulating the activities of global media holdings in order to maintain value-based sovereignty. The author gives a political and economic analysis of value sovereignty, showing the importance of the state as a regulator that allows to eliminate negative informational externalities. Particular attention is paid to the analysis of the international media landscape and the formation of multipolarity in the network space, including the growing phenomenon of technological convergence in the media industry, as well as the positions of individual countries and regions in the global media industry. The corporate structures of the world's largest media holdings are studied and the increasing degree of diversification of their assets is revealed. The generational differentiation of socialization mechanisms in the post-pandemic era, including the proportion of time devoted to social platforms, traditional media (the case of television), as well as the main ways of accessing the Internet and the penetration of new technologies are analysed. The most promising for socialization and fast-growing segments are shown, including Internet TV, virtual reality technologies, video games and cyber-sports. In the final part of the paper the author discusses the main problems and challenges of regulating the national media space in order to ensure value sovereignty in the era of global convergent media.

Key words: values, sovereignty, political economy, information externalities, social platforms, media, convergence, government regulation

Acknowledgements: The publication was prepared as a part of the RFBR-EISI Research Project 21-011-31812 opn "Simulation of the spread of social norms and values: global communications VS information sovereignty of the Russian Federation".

For citation: Degterev, D. A. (2022). Value sovereignty in the era of global convergent media. *Vestnik RUDN. International Relations*, 22(2), 352—371. <https://doi.org/10.22363/2313-0660-2022-22-2-352-371>

С началом COVID-19 и введением карантинных ограничений существенно возросло и без того значительное время, проводимое человечеством у экранов (чаще всего это экраны смартфонов). Современную социально-экономическую модель можно характеризовать как «экономику внимания» (Ray et al., 2020, р. 6) или «когнитивный капитализм» (Нечаев, Белоконов, 2020, с. 115—118), так как большую часть рабочего времени люди находятся перед экранами своих компьютеров и прочих электронных устройств, сосредоточенных преимущественно в мегаполисах.

По состоянию на конец 2020 г., основная часть времени медиапользователей в мире (не менее 7 часов в день) тратится на цифровые устройства (на ТВ — только 3 часа) (рис. 1). Из указанных 7 часов почти 4,5 часа приходятся не на настольный компьютер, а на мобильные приложения.

Таким образом, влияние социальных медиа на потребителей становится практически безграничным. Современный инфорынок — это не только и даже не столько «про бизнес», а скорее про «четвертую власть», ведь он создает наиболее эффективные инструменты

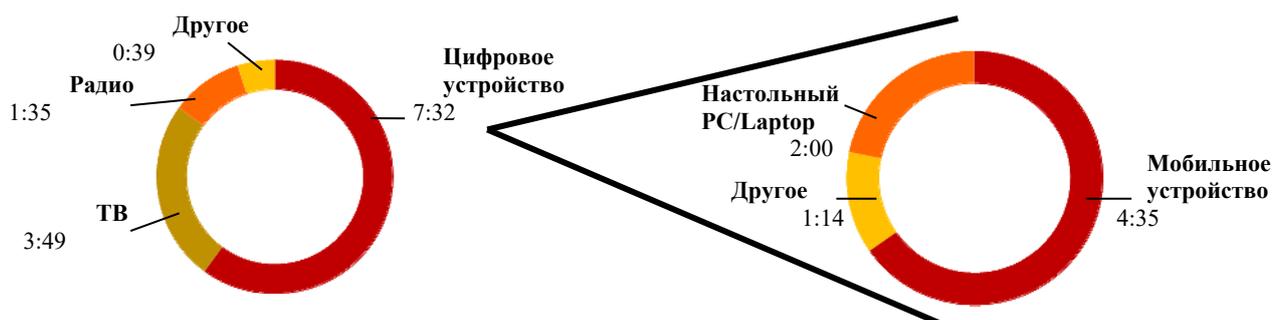


Рис. 1. Время, затрачиваемое на основные медиа
Источник: (PWC, 2020, р. 13).

социализации современного общества. В свою очередь, распространение социальных норм и ценностей — это важнейший элемент формирования общества и трансляции политических установок, а также структурирования потребительского рынка. Наличие глобальных медиаструктур обуславливает необходимость регулирования информационного пространства на национальной территории, однако из-за специфики объекта регулирования это под силу лишь наиболее мощным государствам из числа великих держав.

Постановка проблемы¹

В цифровом пространстве суверенитет в его традиционном понимании (Агамбен, 2011; Шмитт, 2005; Bartelson, 1995; Keohane, 2002; Krasner, 1999; Strange, 1996) преломляется через призму «сетевой власти», которая формируется на нескольких онтологических уровнях (рис. 2) (Зиновьева, 2022, с. 9): 1—2 — базовом (технологическом/инфраструктурном, *hardware*); 3—4 — среднем (программном или сервисном, *software*) и, наконец, 5—7 — содержательном или идеологическом (Yeli, 2017).

¹ Проблема ценностного суверенитета затрагивалась в более ранней работе автора — развернутом экспертном комментарии для РСМД, отдельные части которого использовались при написании данной статьи. См.: Дегтерев Д. А. Распространение социальных норм и ценностей в постпандемийном мире: от реактивного к проактивному подходу // РСМД. 02.02.2022. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/rasprostranenie-sotsialnykh-norm-i-tsennostey-v-postpandemiyom-mire-ot-reaktivnogo-k-proaktivnomu-p/> (дата обращения: 17.02.2022).

На базовом уровне суверенитет государства ограничивается технологической зависимостью от используемого сетевого оборудования — преимущественно европейского (Nokia, Ericsson) либо китайского (Huawei, ZTE)², а также маршрутизаторов (американский Cisco или китайский Huawei).

В рамках «технологической биполярности» (США — КНР) формируются конкурирующие международные режимы управления Интернетом (Дегтерев, Рамич, Пискунов, 2021a; Зиновьева, 2015). При этом ключевую роль, особенно в американской модели, играют мощные цифровые платформы, проводящие информационную политику США в данной сфере (Данилин, 2020; Culpepper & Thelen, 2020).

Значимость сервисов по обработке данных превышает важность программного обеспечения и технической инфраструктуры («нижние этажи», рис. 2) (Зиновьева, 2019, с. 61), что обуславливает развитие понятия «суверенитет данных» (Нечаев, Белоконев, 2020, с. 122). «Большая киберпята» GAFAM (Google, Amazon, Facebook³, Apple, а также Microsoft) использует мощные алгоритмы продвижения идеологически «правильного» контента, а также сокрытия, удаления и блокирования «неправильных» сообщений. Фактически речь идет о формировании «глобальной архитектуры по изменению

² Подробнее см.: RUDN G2 Research Project. URL: <https://g2.rudn.ru/> (accessed: 17.02.2022).

³ 21.03.2022 г. Тверской районный суд г. Москвы удовлетворил иск Генпрокуратуры РФ и признал деятельность соцсети Facebook, принадлежащей Meta, экстремистской, запретив его работу в России.

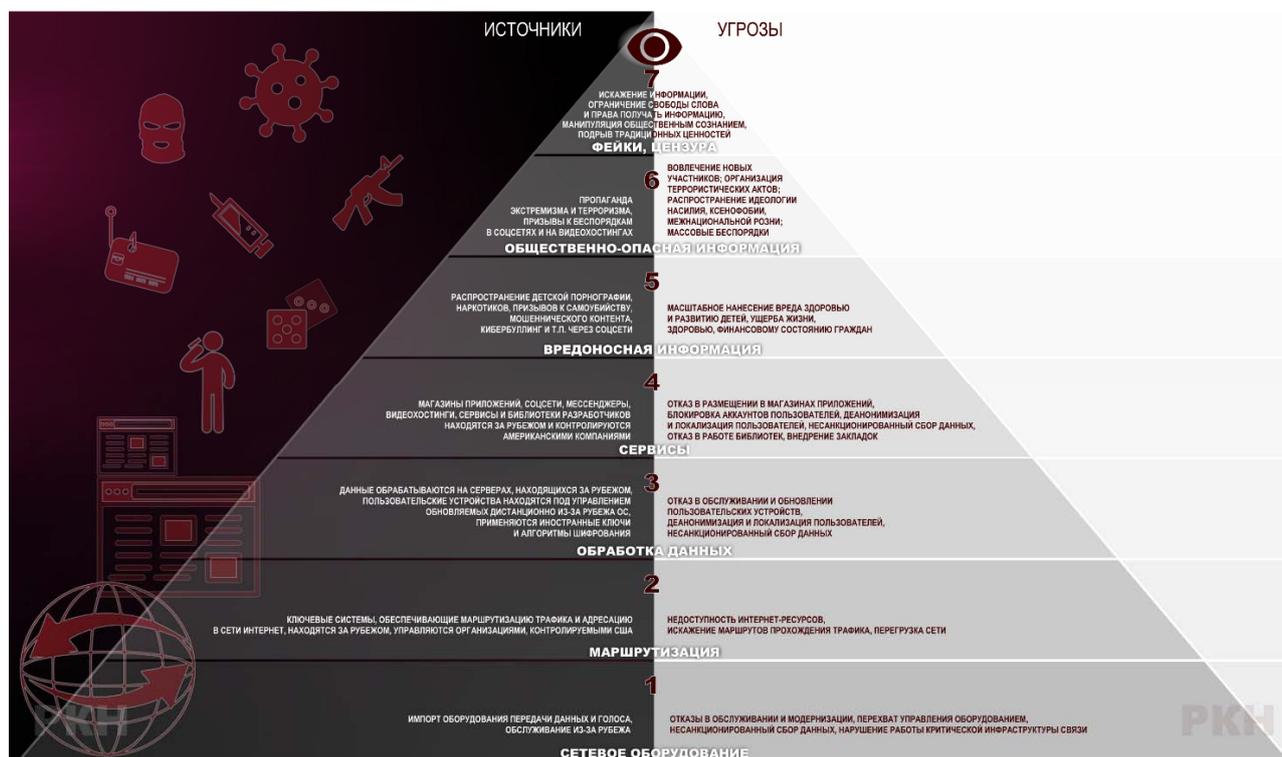


Рис. 2. Пирамида угроз информационной безопасности

Источник: Роскомнадзор. URL: <https://rkn.gov.ru/docs/ugrozy.-piramida.-new-04.02.2021.jpg> (дата обращения: 17.02.2022).

поведения» (Noor, 2020, p. 40) и «цифровом тоталитаризме» (Нечаев, Белоконев, 2020, с. 120).

В рамках стратегий создания вертикально-интегрированных монополий глобальные ИТ-компании стремятся концентрироваться на стратегически более важных «верхних этажах», связанных с созданием и управлением контентом, а не производством «железа». Так, американцы фактически оставили за европейскими производителями нишу сетевого оборудования 5G. Еще одно доказательство — неудачная история покупки Google производителя «железа» Motorola: купили в 2012 г. за 12,5 млрд долл. США, через несколько лет продали за 2,9 млрд долл. США⁴. Amazon из глобальной платформы по электронной коммерции стала ведущим провайдером «облачных хранилищ» данных и публично-облачных вычислений⁵. Соответственно,

⁴ Мартин Р. Слияния и поглощения: не проиграть в лотерею // Harvard Business Review Russia. URL: <https://hbr-russia.ru/management/strategiya/a18140/> (дата обращения: 17.02.2022).

⁵ Кузнецов М., Перемитин Г. Облако и реклама: что помогло акциям Amazon взлететь // Forbes. 04.02.2022.

в глобальном бизнесе становится все выгоднее концентрироваться на хранении, обработке данных и их использовании.

Что касается содержательного уровня проблемы информационного суверенитета, то локальные правила регулирования активности глобальных медиахолдингов для сохранения национальных ценностей ряд экспертов объединяют в коммуникационные режимы (Гасумянов, Комлева, 2020). В последнее время появился целый ряд работ, посвященных непосредственно цифровому суверенитету (Володенков и др., 2021; Зиновьева, 2022; Cuihong Cai, 2020; Lewis, 2020; Pohle & Thiel, 2020; Кутюр, Тоупин, 2020). Достаточно оригинальный подход в этом контексте предлагает С.Н. Федорченко, переносящий основные концепции интеллектуального наследия В.Л. Цымбургского в цифровое пространство (Федорченко, 2021).

Примечательно, что в России первоначальное широкое понятие «информационной

URL: <https://www.forbes.ru/investicii/454613-oblako-i-reklama-cto-pomoglo-akciam-amazon-vzletet> (дата обращения: 17.02.2022).

безопасности» (в мире чаще используется термин «кибербезопасность»), в которое ранее вкладывалась как защита сетевой инфраструктуры и персональных данных, так и ценностная составляющая, в настоящее время уже разделено на две части: собственно «информационная безопасность» в узком смысле (пп. 48—57 Стратегии национальной безопасности) и «защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти» (пп. 84—93 Стратегии)⁶. Во втором случае речь идет как раз о «ценностном суверенитете» в трактовке, близкой, например, к пониманию российского философа и общественного деятеля А.В. Щипкова⁷. Как представляется, второе (*гуманитарное*) направление зачастую является даже более сложным, чем обеспечение собственно информационной безопасности (*технического* направления), в том числе в рамках введения четких требований по локализации контента основных социальных сетей на территории РФ в контексте защиты персональных данных россиян.

В условиях традиционно крепкой связи РФ с европейской и шире — западной культурой (в отличие, например, от КНР) встает вопрос о выделении негативных элементов современной ценностной повестки «коллективного Запада», идущих вразрез с цивилизационной идентичностью РФ. Первые шаги в этом направлении уже сделаны: например, профессор А.В. Лукин (НИУ ВШЭ) провел наглядную деконструкцию основных элементов «новой этики» (Лукин, 2021).

Помимо сложности содержательного выделения негативного контента встает вопрос и об основных каналах его распространения. Например, регулирование контента в ставших уже привычными социальных сетях и мессенджерах — это уже отработанная практика.

⁶ Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Президент России. URL: <http://www.kremlin.ru/acts/bank/47046/> (дата обращения: 17.02.2022).

⁷ Щипков Александр: России необходимо отстаивать «ценностный суверенитет» // Московский Патриархат. 12.10.2021. URL: <http://www.patriarchia.ru/db/text/5851896.html> (дата обращения: 17.02.2022).

Однако как регулировать на территории РФ распространение контента, например, из Clubhouse — социальной сети голосовых сообщений, запущенной в 2020 г.? Или в Pinterest, который продвигает достаточно наглядную инфографику, часть которой откровенно враждебно отражает российскую историю и современность? Или как поступать с Netflix? Вместо уже регулируемых Роскомнадзором каналов информации (и социализации) появляются альтернативные. В какой-то степени в ценностной сфере речь идет о классической «дилемме безопасности» («чем лучше щит, тем сильнее меч», и наоборот) (Дегтерев, 2017, с. 185).

В данной статье предпринята попытка сформулировать основные принципы обеспечения ценностного суверенитета в информационном пространстве в контексте цифровой экономики. Автор отдает отчет в многогранности информационного суверенитета как объекта исследования, и ценностного суверенитета в частности — как предмета данной статьи. Авторский анализ многочисленных детерминант суверенитета может представляться несколько эклектичным, что характерно для оценки многофакторных процессов (например, эклектическая парадигма инвестиционной привлекательности Д. Даннинга). Цифровой суверенитет как результирующую воздействия указанных детерминант ряд авторов называют эмерджентным свойством государства, что присуще сложным социальным системам (Володенков и др., 2021).

На первом этапе (раздел «Политэкономия ценностного суверенитета») идет переосмысление самого понятия ценностного суверенитета в рамках обеспечения общественного благосостояния. Далее («Социализация в условиях конвергенции») показаны основные механизмы социализации индивидуума по мере его взросления в условиях формирования конвергентных медиа. Показано доминирование западных медиа в глобальном медиапейзаже (раздел «Структурная сила Запада в коммуникационной сфере»). Исследуется соотношение сил в информационном пространстве и киберстратегии («техно-национализм») великих держав по обеспечению своего цифрового суверенитета (раздел «Многополярность в

Классификация услуг		
<i>Кто или что является непосредственным объектом обслуживания?</i>		
Характер действия	Люди	Объекты-собственность
Осязаемые действия	Услуги, направленные на человека – Пассажирские перевозки, отели – Охрана здоровья, салоны красоты, физиотерапия, спортклубы – Рестораны, бары – Парикмахерские – Службы ритуальных услуг	Услуги, направленные на физические объекты – Грузовые перевозки – Ремонт и обслуживание – Складское хранение – Розничная торговля – Прачечная и химчистка – Бензозаправка – Благоустройство, отходы, уборка
Неосязаемые действия	Услуги, направленные на сознание человека – Реклама, PR – Искусство и развлечения – Телевидение, связь – Консультационные услуги, образование – Информационные услуги – Музыкальные концерты – Психотерапия, религия	Услуги, основанные на обработке информации – Бухгалтерия, банки – Обработка и передача данных – Страхование, юридические услуги – Программирование и консультации по программному обеспечению (ПО) – Исследования – Операции с ценными бумагами

Источник: (Лавлок, 2005, с. 79).

сетевом пространстве»). В заключительном разделе приводятся выводы по ценностному регулированию в инфопространстве.

Политэкономия ценностного суверенитета

Использование информационно-коммуникационных технологий (ИКТ) связано с оказанием информационных услуг, значительная часть которых относится к «услугам, направленным на сознание человека» (табл. 1, затемненное поле).

Особенностью процесса предоставления данного вида услуг является неосязаемый характер действия, а также необходимость «проникать в сознание человека, формировать его взгляды и влиять на поведение». При этом у клиента возникает своего рода психологическая зависимость от поставщика услуг, для которого появляются возможности для манипуляции, что вызывает необходимость введения определенных этических норм (Лавлок, 2005, с. 81—82).

Зачастую речь идет об использовании Интернета в политических целях, для формирования коллективного самосознания («коллективного подсознательного») пользователей (Зиновьева, 2019, с. 61). Возможность

относительно легко повлиять на сознание миллионов людей ведет к секьюритизации данного пространства. Широкое распространение получают информационные войны — ведущие страны мира создают свои кибервойска для направленного воздействия на сознание жителей других стран, особенно молодежи (Ахмадеев, Бреслер, Манойло, 2021). Опыт «арабской весны» и «цветных революций» показывает, что использование глобальных социальных сетей помимо экономической выгоды несет и существенные политические риски (Lewis, 2020, р. 67). Выделяются и другие политические эффекты «цифровой экономики», связанные с перераспределением возможностей влияния между политическими субъектами (Нечаев, Белоконев, 2020, с. 114—115).

Продвигаемые в национальном медиапространстве ценности непосредственно влияют и на социально-экономическое благосостояние. Ценностное воздействие на функцию полезности потребителей данной страны в конечном счете определяет структуру покупательского спроса и импортных поставок (Дегтерев, 2014, с. 234—245). Странам с крупными внутренними рынками (к числу которых относится и РФ) это позволяет

создавать или, напротив, делать убыточными национальные производства с ежегодным оборотом в десятки миллиардов долларов США.

Ценностная повестка в конечном счете определяет и расстановку приоритетов для целеполагания при стратегическом планировании. В этом контексте речь идет о когнитивном суверенитете, позволяющем «отделять то, что вам действительно нужно, от того, что вам навязано чужими»⁸.

С одной стороны, информационные услуги представляют собой пример обычной бизнес-практики по предоставлению коммерческой информации. С другой стороны, данные рыночные транзакции зачастую оказывают существенное воздействие на третьих лиц, что не находит адекватного отражения в ценах на эти услуги. В экономической науке данное явление называется внешними эффектами (экстерналиями) (Фишер, Дорнбуш, Шмалензи, 1995, с. 236). Наиболее известны отрицательные экстерналии, связанные с размещением экологически грязных производств: владельцы заводов получают завышенную прибыль, в то время как общество несет чистый убыток из-за загрязнения окружающей среды и ухудшения здоровья граждан. Соответственно, задача государства состоит в том, чтобы сделать невыгодным размещение таких вредных производств, вменить их владельцам внедрение зеленых технологий.

В информационной сфере ряд экспертов также разрабатывают проблематику экстерналий (Манохин, 2010). В самом деле, если в рамках сугубо коммерческой услуги (например, платной подписки на международный информационный ресурс) идет дискредитация действующего правительства либо крупных национальных производителей, то благосостояние данной страны, большинства ее граждан существенно сокращается. Налицо чистый убыток общества, не опосредованный рынком, или негативная экстерналия.

⁸ Песков Д. «Остров Россия». Спецпредставитель президента о новой цифровой стратегии // РБК. 09.06.2022. URL: <https://www.rbc.ru/opinions/economics/09/06/2022/62a0e95b9a79472d8b713207> (дата обращения: 10.06.2022).

Соответственно, задача государства как регулятора состоит в том, чтобы «отделить зерна от плевел» — открыть рынки для бизнеса, но закрыть их для политики (Lewis, 2020, p. 71). В этом плане наиболее преуспели китайские регуляторы: с одной стороны, в стране наблюдается взрывной рост популярности стриминговых блогеров, когда за один их онлайн-сеанс реализуются товары на миллиарды долларов. С другой стороны, деятельность таких инфлюэнсеров строго регламентирована и не предполагает распространения негативных для общества норм и ценностей⁹.

В отличие от экологических экстерналий, которые снижают благосостояние всех жителей планеты, информационные, как правило, сокращают благосостояние одного общества, но одновременно увеличивают прибыль другого. Например, введение моды на «заморские товары» снижает сравнительную полезность отечественных товаров и благосостояние местных производителей, но увеличивает объем продаж и прибыль иностранных компаний. Соответственно, у последних появляется соблазн воздействовать на сознание жителей других стран в неокOLONIALном ключе.

Каналов для этого достаточно много — практически любая из услуг, направленных на сознание человека (см. табл. 1), неосвязаема (и, соответственно, сложно контролируема) и достаточно просто может быть сопряжена с негативными информационными экстерналиями. Помимо ТВ, радио и прочих сугубо информационных услуг негативный образ своей страны и ее бизнеса может косвенно формироваться через систему образования и общественных наук, искусство и кинематограф, музыку, неправительственные (НПО) и религиозные организации.

Явные негативные информационные экстерналии купируются посредством введения соответствующих «правил игры». Например, в РФ сформирован Перечень иностранных и международных НПО, деятельность которых

⁹ Журавлева Е. В. Регулирование социальных медиа в КНР // РСМД. 24.01.2022. URL: <https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/regulirovanie-sotsialnykh-media-v-knr/> (дата обращения: 17.02.2022). См. также: (Журавлева, 2022).

признана нежелательной¹⁰; установлено регулирование просветительской деятельности, под которой понимается образовательная деятельность за рамками официальных образовательных программ¹¹.

Однако регулирование собственно ценностной составляющей, имеющей отражение, например, в культуре и искусстве, СМИ и общественных науках, — куда более сложная задача. Какова доля художественного или авторского замысла (в том числе иносказательного), а какова — негативной ценностной составляющей в той или иной статье или произведении искусства? Еще сложнее определить эти доли в полученном гонораре за данное произведение. Если ряд партнерских программ для видеоблогеров (например, от компании Yoola¹²) сопряжены с очевидными негативными информационными экстерналиями для РФ, то в других случаях монетизация антироссийского контента не носит столь явного характера и настраивается посредством уже упомянутых алгоритмов социальных сетей.

Неслучайно в России так тщательно готовятся «Основы государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» — идет доработка законопроекта по итогам общественной экспертизы, проведенной в начале 2022 г.¹³ Многие аналогичные

правила давно введены в КНР, а также Евросоюзе. Так, с 2015 г. под эгидой Европейской службы внешних связей («европейского МИД») действует проект *EUvsDisinfo* «по борьбе с дезинформационными кампаниями РФ», затрагивающими ЕС, государства-члены и соседние страны¹⁴. Ведется мониторинг отдельных публикаций на 15 языках, распространяющих пророссийский нарратив, — отслеживаются авторы и издательства, публикующие данные статьи.

При установлении ценностного суверенитета ряд акторов традиционно выступают за сохранение предыдущих неокOLONиальных укладов, зачастую обосновывая это дороговизной мероприятий по налаживанию эффективной системы регулирования негативных информационных экстерналий. Например, в РФ это наиболее ярко проявилось при имплементации положений «пакета И. Яровой» о хранении персональных данных¹⁵. В самом деле, для отдельных компаний или даже отраслей экономики стоимость установления цифрового и ценностного суверенитета может быть достаточно высокой. Однако чистая прибыль для общества в целом куда более масштабна. В российском случае — это сотни миллиардов долларов США ежегодно. Однако позволить себе данное регулирование может лишь сильное (как в экономическом, так и в технологическом плане) государство.

Социализация в эпоху конвергенции

Процесс социализации индивидуума состоит из нескольких этапов (рис. 3). Первичная социализация проходит в детстве (до 9 лет), в подростковом возрасте (с 9 до 15 лет), а также в молодости (с 16 до 18 лет), при этом уже в детстве личность человека формируется

¹⁰ Перечень иностранных и международных неправительственных организаций, деятельность которых признана нежелательной на территории РФ // Министерство юстиции РФ. 31.05.2022. URL: <https://minjust.gov.ru/ru/documents/7756/> (дата обращения: 09.06.2022).

¹¹ Федеральный закон от 05.04.2021 № 85-ФЗ «О внесении изменений в Федеральный закон “Об образовании в Российской Федерации”» // Официальный интернет-портал правовой информации. 05.04.2021. URL: <http://publication.pravo.gov.ru/Document/View/0001202104050036> (дата обращения: 09.06.2022).

¹² Моргенштерна внесли в иноагенты за политическую деятельность и сотрудничество с Yoola Labs // BFM.RU. 07.05.2022. URL: <https://www.bfm.ru/news/499450> (дата обращения: 09.06.2022).

¹³ Проведение общественного обсуждения уведомления при разработке проекта нормативного правового акта «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» // Федеральный портал проектов нормативно-правовых актов.

URL: <https://regulation.gov.ru/projects#npa=123967> (дата обращения: 09.06.2022).

¹⁴ EUvsDisinfo. URL: <https://euvsdisinfo.eu/> (accessed: 09.06.2022).

¹⁵ Кинякина Е. Цена закона: почему «пакет Яровой» обойдется в 45 млрд рублей // Forbes. 14.05.2018. URL: <https://www.forbes.ru/tehnologii/361401-cena-zakona-pochemu-paket-yarovoy-oboydetsya-v-45-mlrd-rublej> (дата обращения: 09.06.2022).



Рис. 3. Основные этапы процесса социализации

Источник: Кулинич А. Механизмы социализации личности — что это, виды // Srazupro. URL: <https://srazu.pro/socializacia/mexanizmy-socializacii-lichnosti.html> (дата обращения: 17.02.2022).

Таблица 2

Основные институты социализации

Традиционные институты	Традиционные СМИ	Новые медиа	Новейшие медиа
– Семья	– ТВ	– Социальные сети	– Мессенджеры
– Религия	– Радио	– LiveJournal	– TikTok
– Школа	– Газеты	– YouTube	– Подкасты

Источник: составлено автором.

на 70 %. Вторичная социализация происходит в период зрелости (с 18 до 50 лет) и после него¹⁶.

Существуют различные институты социализации (табл. 2), при этом со временем меняется их относительная важность — все более важную роль начинают играть «новейшие медиа», связанные с цифровыми сервисами, — мессенджеры (Telegram, WhatsApp, Viber), TikTok и подкасты.

Представители разных поколений (по адаптированной классификации Штрауса — Хау (Strauss & Howe, 1997)) — зумеры или

хоумлендеры (рожденные после 2003 г.); миллениалы (рожденные в 1985—2002 гг.); поколение X (рожденные в 1964—1984 гг.) и бэби-бумеры (рожденные в 1944—1963 гг.)¹⁷ — имеют отличающиеся друг от друга предпочтения по основным каналам социализации (рис. 4).

Так, если среди поколения бэби-бумеров (1944—1963 г.р.) ежедневно на просмотр телевидения и аналогичные форматы в 2016—2017 гг. затрачивалось почти по

¹⁶ Кулинич А. Механизмы социализации личности — что это, виды // Srazupro. URL: <https://srazu.pro/socializacia/mexanizmy-socializacii-lichnosti.html> (дата обращения: 17.02.2022).

¹⁷ RuGenerations — Российская школа теории поколений. URL: <https://rugenerations.ru/> (дата обращения: 17.02.2022).

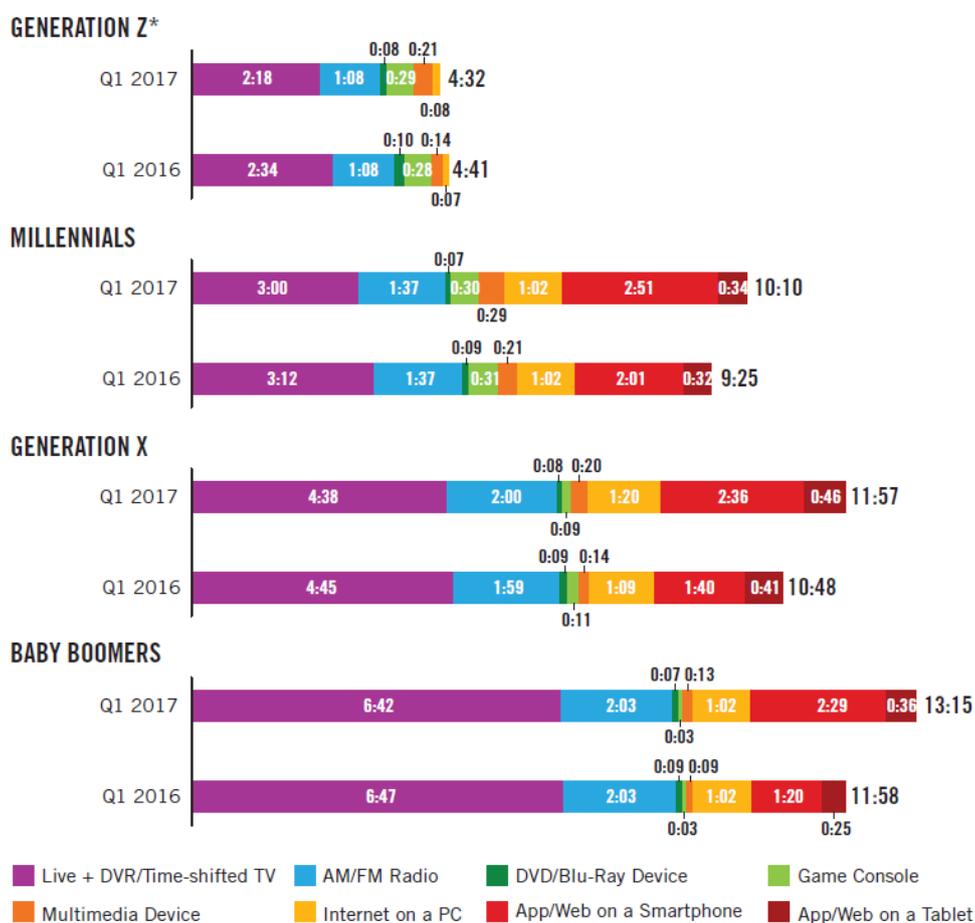


Рис. 4. Среднее время (в часах), затрачиваемое на разные виды медиа

Источник: (Turow, 2020, p. 323).

7 часов времени, а на слушание AM/FM радиостанций — почти по 3 часа, то далее эта доля существенно сокращается. У поколения X (1964—1984 г.р.) — уже по 4 и 2 часа, у поколения миллениалов (Y) (1985—2002 г.р.) — уже по 3 и 1,5 часа, а у поколения зумеров (Z) (с 2003 г. по н.в.) — всего 2 и 1 час соответственно. При этом поведенческие паттерны у одного поколения со временем не сильно изменяются, а вот различия между поколениями очень существенны. Наибольшее количество часов за просмотром Интернета в смартфонах наблюдается у поколения миллениалов (в 2017 г. достигало 2,5 часов в день) (Turow, 2020).

Поскольку первичная социализация происходит в раннем возрасте, она затрагивает преимущественно зумеров, а также миллениалов и проводится с учетом специфики используемых ими институтов социализации. Данные группы, прошедшие социализацию

преимущественно в киберпространстве, лучше адаптированы к вызовам цифровой экономики, чем старшие, «аналоговые» поколения (Нечаев, Белоконев, 2020, с. 117). Эффект социализации усиливается, если для нее используется одновременно несколько институтов (см. табл. 2), что позволяет закрепить информационный контент традиционными способами. Успешным проектом такого рода являются «Киноуроки в школах России», когда при поддержке школьных учителей идет выработка социальных практик по ценностям, показанным в фильмах¹⁸.

¹⁸ Подробнее см.: Панельная сессия 2. Проблема ценностей на Евразийском пространстве и механизмы их распространения. VII Международная конференция «Внешняя политика России на евразийском пространстве». РУДН, 10.12.2021 г. // Youtube. URL: <https://www.youtube.com/watch?v=XfL3ajY6zpA> (дата обращения: 17.02.2022).

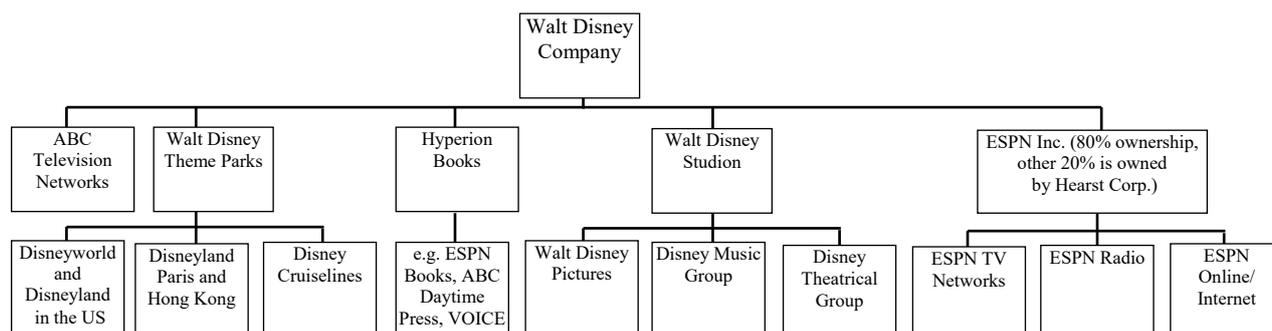


Рис. 5. Организационная структура медиахолдинга Walt Disney

Источник: (Turrow, 2020, p. 174).

Глобальные медийные холдинги занимают сегодня интернет-видео, интернет-рекламой и интернет-новостями, кинопроизводством, ТВ, радио, издательской (газеты, журналы, книги), развлекательной деятельностью (видеоигры), а в последние пару лет — и технологиями дополненной (виртуальной) реальности. Главное — это контент, для распространения которого используются самые современные технологии и каналы продаж, в первую очередь в рамках сети Интернет. При этом ключевую роль начинают играть не официальные медиа, а популярные блогеры (в том числе детские) в рамках адаптированной к современным реалиям теории двухступенчатого потока информации Э. Каца (Katz, 1957).

Широкое распространение в медиа получил феномен конвергенции, связанный с повсеместным распространением ИКТ и формированием унифицированных коммуникаций (Зиновьева, 2019, с. 61). Речь идет о технологии OTT (Over the Top), то есть предоставлении видеослужб в цифровом формате через Интернет, а не через привычный канал телевидения.

Анализ корпоративных структур крупнейших медиахолдингов мира показывает большую степень диверсификации их активов. Например, компания «Уолт Дисней» (4—5-е место в мире), специализирующаяся на социализации детей, включает в себя такие разные активы, как телеканал ABC, а также ESPN, сеть радиостанций и онлайн-сервисов ESPN, тематические парки Walt Disney, издательство Hyperion Books, а также анимационную студию (ранее — главный актив) (рис. 5).

Кросс-культурные различия в инструментах социализации населения различных

стран связаны с уровнем проникновения сети Интернет, а также доступом к основным онлайн-приложениям. Поскольку уровень распространения персональных компьютеров в странах «Глобального Юга» крайне невысок, основным инструментом для доступа в Интернет выступают как раз мобильные телефоны. В этом контексте особое значение приобретает тот факт, имеют ли мобильные телефоны достаточный функционал для использования Интернета, в том числе удобного функционирования основных онлайн-приложений. В странах «Глобального Юга» распространение смартфонов (наиболее современных моделей телефонов, позволяющих осуществлять максимально широкое функционирование большинства онлайн-сервисов) неравномерно (см. рис. 5): от 86 % населения в Ливане до всего 32 % — в Индии¹⁹.

Пандемия COVID-19 также существенно повлияла на мировой медиаландшафт, изменив каналы распространения информации и фактически ускорив сокращение доли традиционных медиа (рис. 6). Снижается выручка печатных СМИ и традиционных телеканалов, а также сетей кинотеатров. Больше всего растет сегмент создания виртуальной реальности, предоставления видеослужб через Интернет (уже упоминавшийся OTT), видеоигр и электронного спорта.

Особое внимание также привлекает сегмент подкастов, то есть процесс создания

¹⁹ Silver L. et al. Use of Smartphones and Social Media Is Common Across Most Emerging Economies // Pew Research Center. March 7, 2019. URL: <https://www.pewresearch.org/internet/2019/03/07/use-of-smartphones-and-social-media-is-common-across-most-emerging-economies/#table> (accessed: 17.02.2022).

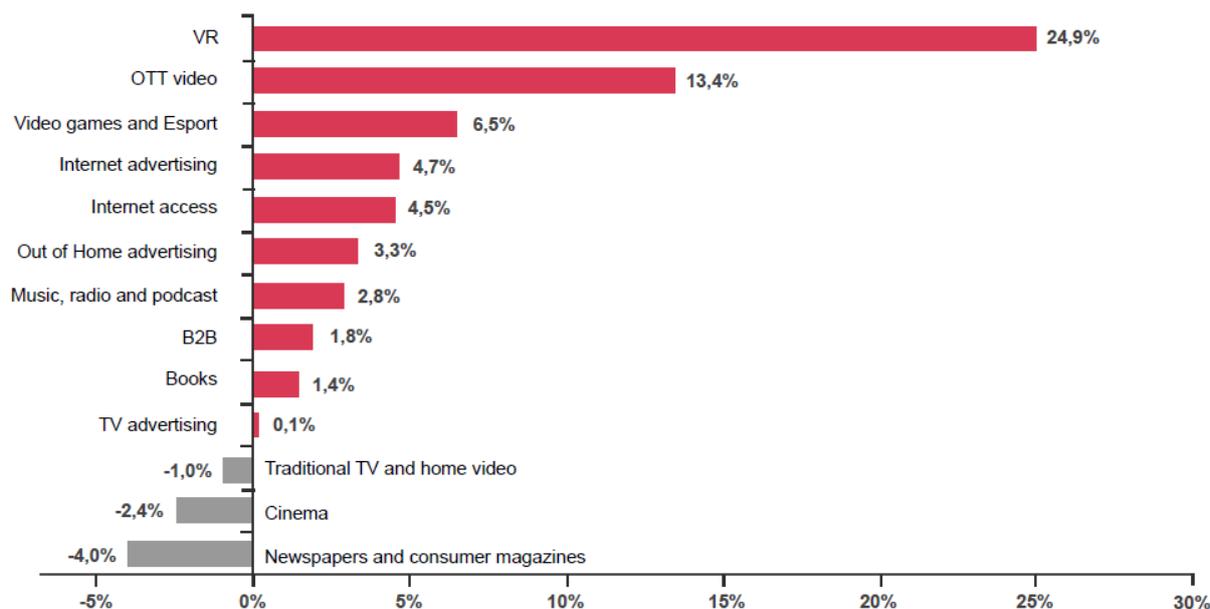


Рис. 6. Совокупные среднегодовые темпы роста в основных сегментах отрасли глобальных развлечений и медиа в 2020 г.

Источник: (PWC, 2020, p. 14).

Global podcast advertising revenue (US\$m) and monthly listeners (mn), 2015-2024

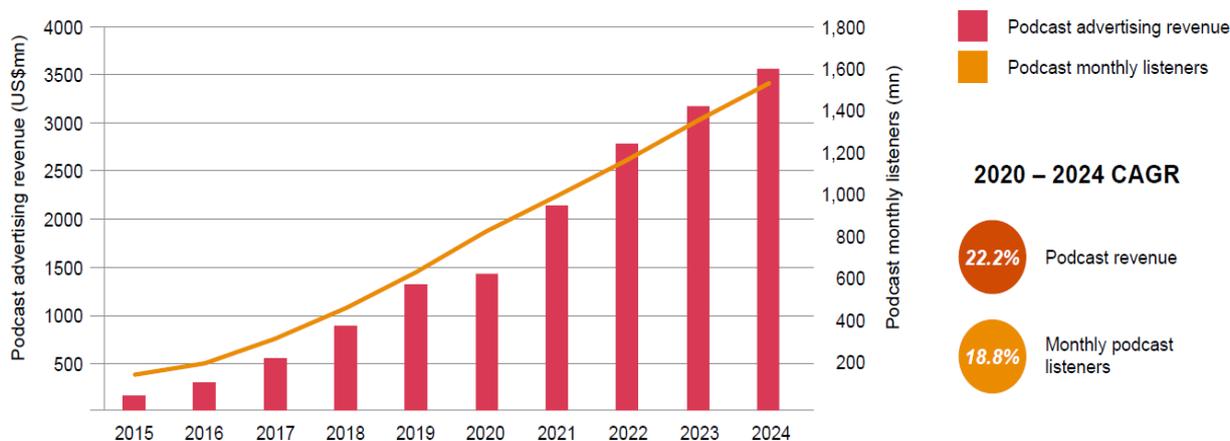


Рис. 7. Рекламные доходы и аудитория подкастов в 2015—2024 гг.

Источник: (PWC, 2020, p. 19).

и распространения звуковых или видеофайлов в стиле радио- и телепередач в Интернете (близкий к уже обозначенному формату OTT). За время пандемии наблюдался устойчивый рост как рекламной аудитории, так и количества слушателей подкастов (рис. 7).

Сервис подкастов позволяет максимально кастомизировать предлагаемый информационный продукт, приводя к формированию транстерриториальных социальных и политических движений, которые возникают на

основе общих (и достаточно узкоспециализированных) ценностей и интересов (Нечаев, Белоконов, 2020, с. 119).

Структурная сила Запада в коммуникационной сфере

В терминах международной политической экономики можно говорить о структурной силе «коллективного Запада» в коммуникационной сфере, которую (по С. Стрэндж)

условно можно отнести к одной из составляющих «структуры знаний» (*knowledge structure*) — четвертой структурной власти «первого уровня» наравне с безопасностью, производством и финансами (Strange, 1994, pp. 119—138). Фактически речь идет о глобальных самоокупаемых системах по воспроизводству западных социальных норм и ценностей.

Возникший под эгидой Агентства передовых оборонных исследований США (DARPA) Интернет (ARPA-net) первоначально представлялся как «ничья земля», «всеобщее благо», а киберпространство пытались наделить «цифровой исключительностью» и объявить неподвластным национальным границам (Зиновьева, 2022, с. 8—13). Доминирование в цифровой экономике первых социальных платформ из Калифорнии (США), а среди первых пользователей Интернета — жителей западных стран наложилось на «однополярный момент» в мировой политике, поэтому американские подходы к регулированию глобальной сети первоначально не оспаривались. Более того, если в 2009 г. в мире существовало почти два десятка социальных сетей, которые были национальными лидерами как в западных, так и незападных странах, то впоследствии почти всех их вытеснила американская сеть Facebook (рис. 8). США заставили отказаться от амбиций на существование собственных социальных сетей даже своих союзников, взяв курс на создание технологической гегемонии и извлечение связанной с этим суперренды (Cuihong Cai, 2020, p. 49).

В большинстве стран постсоветского пространства между тем лидирует российская «ВКонтакте» (VK), а в более традиционных обществах (Молдавия, Грузия, Туркменистан, Узбекистан, Таджикистан) долгое время также доминировали российские «Одноклассники». В КНР и Иране применяется административный запрет на Facebook, поэтому в КНР на первое место вышла сеть *QZone* (разработка китайской компании Tencent, ныне — QQ), получил распространение также мессенджер *WeChat* и сервис микроблогов *Weibo*, а в Иране (в отсутствие собственных конкурентных разработок) — другая американская со-

циальная сеть Instagram (21.03.2022 г. Тверской районный суд г. Москвы удовлетворил иск Генпрокуратуры РФ и признал деятельность соцсети Instagram, принадлежащей Meta, экстремистской, запретив ее работу в России. — *Прим. ред.*).

Американское доминирование в киберпространстве усиливается и лидерством поисковика Google, на который, по ряду оценок, приходится свыше 90 % всех запросов в сети Интернет. Лишь в нескольких странах Google не является монополистом, в том числе в РФ (делит лидерство с «Яндексом»), КНР (доминирует Baidu) и США (чуть более 10 % рынка приходится на Bing (от Microsoft), Yahoo! и DuckDuckGo)²⁰. Фактически речь идет о «монополии на правду», глобальном контроле над информацией и информационным обществом либо об уже упоминавшемся цифровом тоталитаризме, ведь 90 % интернет-пользователей в мире получают тот ответ на поисковый запрос, который выдает им компания Google, и подвержены влиянию алгоритмов Facebook, а также YouTube.

В контексте медиаконвергенции социальные платформы интегрированы в крупные коммуникационные холдинги, включающие как традиционные СМИ (газеты, телевидение), так и новые интернет-медиа. С 2007 г. американское коммуникационное агентство *ZenithOptimedia* готовило рейтинг крупнейших владельцев глобальных медиа (табл. 3), ранжируя их по доходам от рекламы. Последний такой рейтинг выходил в 2017 г.

Из данных табл. 3 видно, что в 2013 г. в ТОП-30 восходящие державы были представлены лишь двумя латиноамериканскими телеканалами. В 2015 г. началось «продвижение» китайской поисковой системы *Baidu* и китайского телеканала CCTV. В 2017 г. к ним добавилась и китайская корпорация *Tencent*, поддерживающая сервисы обмена быстрыми сообщениями QQ и WeChat.

Схожий рейтинг медиаконцернов мира с 2007 г. готовит немецкий Институт медиа-

²⁰ Search Engine Market Share Worldwide 2022 // Statcounter Global Stats. URL: <https://gs.statcounter.com/search-engine-market-share#yearly-2022-2022-bar> (accessed: 13.06.2022).

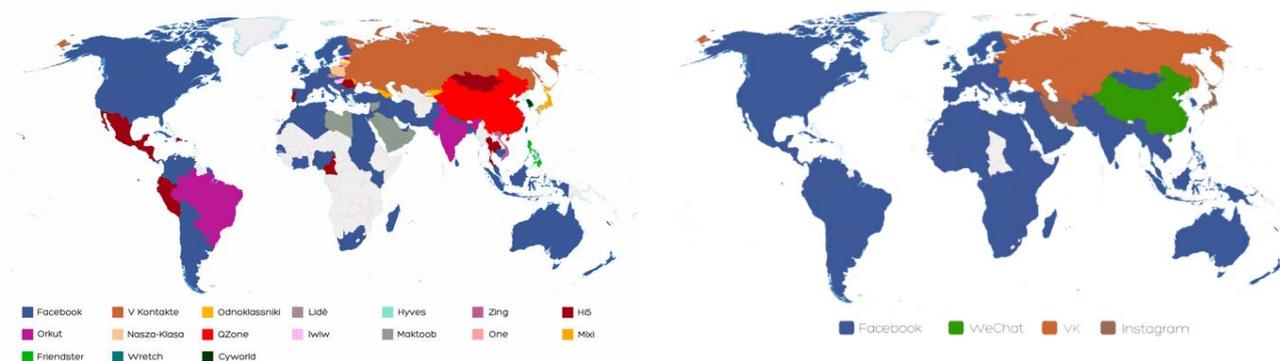


Рис. 8. Лидирующая социальная сеть по странам мира в июне 2009 г. (слева) и в январе 2022 г. (справа)
 Источник: World Map of Social Networks. URL: <http://vincos.it/world-map-of-social-networks/> (accessed: 17.02.2022).

Таблица 3

ТОП-30 глобальных медиа в 2013—2017 гг.

№ п/п	2013		2015		2017	
	Компания	Страна	Компания	Страна	Компания	Страна
1	Google	США	Google	США	Alphabet (Google)	США
2	DirectTV	США	Walt Disney	США	Facebook	США
3	News Corp.	Австрал.	Comcast	США	Comcast	США
4	Walt Disney	США	XXI Century Fox	США	Baidu	КНР
5	Comcast	США	CBS Corp.	США	Walt Disney	США
6	Time Warner	США	Bertelsmann	ФРГ	XXI Century Fox	США
7	Bertelsmann	ФРГ	Viacom	США	CBS Corp.	США
8	Cox Enterprises	США	Time Warner	Великобр.	iHeartMedia	США
9	CBS Corp.	США	News Corp.	ФРГ	Microsoft	США
10	BSkyB	Великобр.	Facebook	США	Bertelsmann	ФРГ
11	Viacom	США	Advance Publ.	США	Viacom	США
12	Vivendi	Франция	iHeartMedia	США	Time Warner	США
13	Advance Publ.	США	Discovery	США	Yahoo	США
14	Clear Channel Com	США	Baidu	КНР	Tencent	КНР
15	Yahoo!	США	Gannett	США	Hearst	США
16	Gannett	США	Asahi Shimbun Com	Япония	Advance Publications	США
17	Globo	Бразилия	Grupo Globo	Бразилия	JCDecaux	Франция
18	Grupo Televisa	Мексика	Yahoo!	США	News Corp.	США
19	Fuji Media Hold.	Япония	Fuji Media	Япония	Grupo Globo	Бразилия
20	Yomiuru Holdings	Япония	CCTV	КНР	CCTV	КНР
21	Axel Springer	ФРГ	Microsoft	США	Verizon	США
22	Mediaset	Италия	Hearst Corp.	США	Mediaset	Италия
23	Hearst Corp.	США	JCDecaux	Франция	Discovery	США
24	JCDecaux	Франция	Yomiuru Hold.	Япония	TEGNA	США
25	Asahi Shimbun Com	Япония	Mediaset	Италия	ITV	Великобр.
26	Microsoft	США	Axel Springer	ФРГ	ProSiebenSat	ФРГ
27	Facebook	США	ITV plc	Великобр.	Sinclair Broadcasting	США
28	ProSiebenSat	ФРГ	ProSiebenSat	ФРГ	Axel Springer	ФРГ
29	ITV plc	Великобр.	NTV	Канада	Scripps Networks Int	США
30	Sanoma	Финлянд.	Sanoma	Финлянд.	Twitter	США

Примечание. Затемнены показатели по восходящим державам.

Источник: Chinese Companies Enter Top 30 Global Media Owners for First Time // ZenithOptimedia. May 6, 2014. URL: <https://www.zenithmedia.com/chinese-companies-enter-top-30-global-media-owners-for-first-time/> (accessed: 13.06.2022); Here Are the World's Top Earning Media Owners // Marketing-Interactive. May 11, 2015. URL <https://www.marketing-interactive.com/top-30-earning-media-owners-globally> (accessed: 13.06.2022); Google and Facebook Now Control 20% of Global Adspend // ZenithOptimedia. 2017. URL https://www.zenithusa.com/wp-content/uploads/2017/06/Top-30-Global-Media-Owners-2017_Press-Release_US.pdf (accessed: 13.06.2022).

Таблица 4

ТОП-10 новостных медиакомпаний англоязычной среды в 2019 г.

№ п/п	Компания	Страна	Бренды	Общий доход, млрд долл. США	Доход от новостного/информ. бизнеса, млрд долл. США
1	Alphabet	США	Google, Google News, YouTube	161,9	150,0
2	Facebook	США	Facebook, Instagram, WhatsApp	70,7	69,7
3	Apple	США	Apple News, Apple News+, Apple TV, Apple One	260,2	53,8
4	Walt Disney	США	ESPN, National Geographic, ABC, Viceland	65,4	28,4
5	Comcast	США	MSNBC, NBC Sky, Sky News	108,9	25,5
6	ViacomCBS	США	CBS, Chanel 5, MTV	27,8	24,4
7	Netflix	США	Netflix	20,2	20,2
8	Amazon	США	Amazon Prime Video, Kindle, Audible, Twitch	280,5	19,2
9	ByteDance	КНР	TikTok	16,0	16,0
10	Microsoft	США	MSN, LinkedIn	143,0	15,8

Источник: Turvill W. The News 50: Tech Giants Dwarf Rupert Murdoch to Become the Biggest News Media Companies in the English-Speaking World // PressGazette. December 3, 2020. URL: <https://www.pressgazette.co.uk/biggest-media-companies-world/> (accessed: 17.02.2022).

коммуникационной политики. В рейтинге 2020 г. на 4-м месте находится китайская компания *Tencent* с выручкой в 61 млрд евро, на 9-м — *ByteDance* (разработчик сервиса коротких видеосообщений TikTok) с выручкой в 32 млрд евро, на 11-м — Шанхайская медиагруппа (28 млрд евро), на 22-м — *Baidu* (14,3 млрд евро)²¹.

Кроме развлекательного контента на формирование ценностей большое влияние оказывает новостная и информационная повестка, продвигаемая ведущими мировыми холдингами, в том числе на английском языке, который выступает языком международного общения (табл. 4).

Помимо подавляющего доминирования США в данном рейтинге (9 из 10 компаний) следует отметить и «конвергентный» характер бизнеса основных участников, подробно рассмотренный в предыдущем разделе (Ciasullo, Troisi & Cosimato, 2018). Так, провайдерами информационного (а следовательно, и ценностного) контента выступают как социальные платформы (Alphabet, Facebook, ByteDance), создатели мультфильмов и фильмов (Walt Disney, Netflix), дистрибьюторы

контента (Amazon), так и разработчики программного обеспечения и компьютеров (Microsoft, Apple), а также представители индустрии кабельного телевидения (Comcast, ViacomCBS). Все они — ключевые акторы глобального информационного общества (Зиновьева, 2019, с. 83—92), «кующие» структурную силу «коллективного Запада» в медиасфере.

Многополярность в сетевом пространстве

Интернет представляет собой новое мировое политическое пространство (Международные отношения России..., 2011), режимы управления которым находятся на стадии определения повестки дня, а взаимодействие основных акторов — в процессе торга (Зиновьева, 2019, с. 36). Идет активное конструирование международно-правовых режимов, причем лишь часть мировых акторов (США, КНР, ЕС и РФ) можно отнести к *rule-makers* (то есть к тем, кто формирует «правила игры»), остальные («маргинальное большинство») — к *rule-takers*. Таким образом, в киберпространстве формируется такая же иерархичная система, как и в традиционном политическом пространстве (Дегтерев, Рамич, Цвык, 2021b, с. 215).

Легитимные усилия национальных государств по установлению суверенитета в

²¹ Die 50 größten Medien- und Wissenskonzerne 2020 // Institut für Medien- und Kommunikationspolitik. 2021. URL: <https://www.mediadb.eu/de/datenbanken/internationale-medienkonzerne.html> (accessed: 17.02.2022).

киберпространстве еще несколько лет назад всячески стигматизировались. Так, в 2016 г. в журнале *The Economist* был введен термин «балканизация Интернета» (Зиновьева, 2022, с. 11), то есть подразумевалось, что формирование национальных сегментов глобальной сети сродни неконтролируемому и кровавому хаосу распада Югославии. В этом же ключе следует рассматривать и широко распространенный термин «техно-национализм» (Cuihong Cai, 2020): последовательная национальная политика в области информационной безопасности отождествлялась чуть ли не с фашизмом.

Однако, несмотря на подавляющее превосходство США, описанное в предыдущем разделе, либеральный киберинтервенционизм постепенно начал пробуксовывать. Ключевую роль в этом сыграли Китай и Российская Федерация, способствовавшие формированию многополярности в информационной сфере.

В КНР были созданы мощные ИТ-холдинги — Baidu, Alibaba, Tencent, and Xiaomi (BATX), фактически выступившие действенной альтернативой американской «пятерке» GAFAM и бросившие вызов информационной «структурной силе» «коллективного Запада». На сегодняшний день крупнейшим и, пожалуй, наиболее стремительным успехом незападной медиакомпании, в том числе и в западном медиaprостранстве, является ByteDance. Ее сервисом TikTok в настоящее время пользуются более 2 млрд чел. в мире, а выручка по итогам 2021 г. достигла 58 млрд долл. США²², выводя ее в ТОП-5 мировых медиакомпаний. Успех компании встревожил американских медиарегуляторов, которые стали говорить о возможности блокирования компании в западных странах, а сама компания — о продаже своего американского бизнеса компании Oracle, однако после ухода Д. Трампа она сменила состав ключевых акционеров (вошел ряд американских фондов) и управляющих, но продолжила работу в США²³.

²² Котченко К. Выручка владельца TikTok увеличилась на 70 % за 2021 год. Рост замедлился // РБК. 20.01.2022. URL: https://quote.rbc.ru/news/short_article/61e95d1a9a794713e519eb30 (дата обращения: 17.02.2022).

²³ Gerstein J. ByteDance Is Walking Away from Its Tiktok Deal with Oracle Now That Trump Isn't in Office,

В КНР были приняты наиболее проработанные правила регулирования национального Интернета, реализована стратегия «сильного сетевого государства», а вопросы обеспечения информационной безопасности и «интернет-суверенитета» стали приоритетами национальной безопасности²⁴. Китай первым показал, что всей мощи западной структурной медиасилы можно противопоставить последовательные усилия по отстаиванию своего информационного суверенитета, что «новая этика» — это не объективная социальная реальность, а пропаганда псевдонаучных теорий, с которыми можно и нужно бороться (Лукин, 2021). Обеспечив собственный ценностный (и шире — информационный) суверенитет, КНР приняла активное участие в создании альтернативных американским правил управления глобальным Интернетом (Дегтареv, Рамич, Пискунов, 2021a).

В целом китайскую стратегию эксперты называют *оборонительным техно-национализмом с независимостью и сотрудничеством* (упор на собственные технологические разработки), в то время как американскую — *наступательным техно-национализмом с односторонним гегемонизмом* (Cuihong Cai, 2020). Прослеживается прямая аналогия с двумя подходами реалистической парадигмы — оборонительным К. Уолтца (акцент на обеспечение собственной безопасности) и наступательным Дж. Миршаймера (максимизация собственной мощи) (Mearsheimer, 2014).

На первом этапе страны «коллективного Запада» представляли китайский кейс скорее как аберрацию, которой не должен был следовать «свободный мир». В РФ изначально не вводилось жестких ограничений относительно использования глобальных социальных платформ. В свободной конкурентной борьбе

Report Says // BusinessInsider. February 15, 2021. URL: <https://www.businessinsider.com/bytedance-ending-oracle-deal-because-trump-is-out-scmp-2021-2> (accessed: 17.02.2022).

²⁴ Журавлева Е. В. Регулирование социальных медиа в КНР // РСМД. 24.01.2022. URL: <https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/regulirovanie-sotsialnykh-media-v-kr/> (дата обращения: 17.02.2022). См. также: (Понька, Рамич, У, 2020).

российские разработчики социальных платформ «ВКонтакте», «Одноклассники», Telegram и интернет-сервисов («Яндекс», «Озон» и др.) на равных конкурировали с глобальными компаниями, укрепляя тем самым информационный суверенитет России. Проект П. Дурова Telegram стал самым быстрорастущим приложением 2021 г. в мире²⁵, являя собой прообраз структурной силы не-Запада в области коммуникаций. Все большее количество пользователей в РФ, странах Азии и Африки, а также в западных странах, включая США, выбирают данный мессенджер как альтернативу «конвенциональным» западным продуктам.

Россия приняла активное участие в разработке принципов международной информационной безопасности на основе суверенного равенства в рамках БРИКС и ШОС, инициировала работу Группы правительственных экспертов ООН (ГПЭ), а также Рабочую группу ООН открытого состава (РГОС) по вопросам безопасности в сфере использования ИКТ на период 2021—2025 гг.

В ЕС формируется несколько иная модель регулирования цифрового пространства и продвижения ценностей (Roberts et al., 2021; Burwell & Propp, 2020), которую можно охарактеризовать как *оборонительный технонационализм с многосторонним сотрудничеством* (Cuihong Cai, 2020, pp. 50—51).

В то же время в странах Азии и Африки постепенно увеличивалось число интернет-пользователей, составляющих большинство уже на данный момент. Естественно, продвигаемые в сети западнцентричные нарративы мало соответствовали традиционным ценностным установкам новых пользователей (Noor, 2020, p. 39).

Однако «последний гвоздь в крышку» «свободного Интернета» забили сами американцы, которые ввели максимально жесткие правила интернет-цензуры во время президентских выборов 2020 г. и заблокировали

Twitter Д. Трампа²⁶. Власти США обосновали данные меры необходимостью бороться с дезинформацией для обеспечения законности выборов (Ray et al., 2020, p. 7), то есть ровно тем же, чем руководствовались незападные страны, устанавливая национальные правила информационной безопасности.

По мере формирования национальных режимов обеспечения информационной безопасности и интернет-суверенитета эксперты стали все больше говорить о регионализации глобальной сети (Зиновьева, 2019, с. 64—68) и формировании «технологических островов»²⁷. Данный процесс только ускорился после обострения ситуации на Украине в феврале 2022 г. Из-за нежелания блокировать призывы к насилию в отношении граждан РФ и Белоруссии компания Meta (социальные сети Facebook и Instagram) 21 марта 2022 г. была признана экстремистской, а ее деятельность запрещена на территории РФ²⁸.

Как представляется, это отражение более долгосрочной тенденции на технологический декаплинг, связанный с формированием «новой биполярности», созданием замкнутых контуров «коллективного Запада» и «коллективного не-Запада» (Дегтерев, Рамич, Цвык, 2021b). Данные тенденции будут только усиливаться, ведь украинский кризис — это локальное противостояние в глобальном «транзите власти» (США — КНР). Секьюритизация информационного пространства, использования его в военных целях для воздействия на население противника будет пресекаться основными конфликтующими сторонами, что будет приводить к формированию новых информационных барьеров.

²⁶ Полякова В. Twitter навсегда заблокировал аккаунт Трампа // РБК. 09.01.2021. URL: <https://www.rbc.ru/politics/09/01/2021/5ff8f6599a7947cb28665d7e> (дата обращения: 17.02.2022).

²⁷ Песков Д. «Остров Россия». Спецпредставитель президента о новой цифровой стратегии // РБК. 09.06.2022. URL: <https://www.rbc.ru/opinions/economics/09/06/2022/62a0e95b9a79472d8b713207> (дата обращения: 10.06.2022).

²⁸ Локотецкая М. Суд признал Meta экстремистской организацией и запретил на территории России // ВФМ. 21.03.2022. URL: <https://bfm-ru.turbopages.org/bfm.ru/s/news/495697> (дата обращения: 10.06.2022).

²⁵ Bikker G. 2021: The Year The World Is Set to Spend \$135 Billion Dollars – In Mobile Apps and Games in New Record // Data.Ai. December 8, 2021. URL: <https://www.data.ai/en/insights/market-data/2021-end-year-mobile-apps-recap/> (accessed: 17.02.2022).

Выводы

В современную цифровую эпоху ускорились процессы конвергенции между традиционными СМИ (ТВ, радио, пресса) и новыми интернет-медиа (социальные платформы, блоги, подкасты). Цифровое пространство многократно усиливает информационное воздействие, а его использование становится основным механизмом социализации населения. В сложившихся условиях критическую важность приобретает обеспечение информационного, в том числе ценностного, суверенитета, представляющего собой комплексный процесс, включающий технологическую, программную и содержательную составляющие.

Если в первые годы развития Интернета, пришедшиеся на «однополярный момент», киберпространство представляли как «ничью землю» и «всеобщее благо» (по факту — это была монополия гегемона), то на сегодняшний день дискурс о недопущении «балканизации» Интернета уже не актуален. Большинство ведущих стран мира перешли к созданию собственных режимов обеспечения информационного суверенитета. В текущих реалиях стоит вопрос сопряжения различных глобальных подходов к обеспечению информационной безопасности (Lewis, 2020, p. 65).

В условиях подавляющего доминирования стран «коллективного Запада» в глобальном медиапространстве (коммуникационная структурная сила) западные страны используют асимметричные стратегии — национальные модели регулирования информационного контента, развивая много-

полярность в сетевом пространстве. Например, наиболее проработанная («трехступенчатая») модель регулирования социальных сетей сложилась на сегодняшний день в КНР²⁹. Соседи РФ по постсоветскому пространству также используют свои механизмы регулирования контента в социальных сетях³⁰ и формируют собственные коммуникационные режимы (Бегалинова и др., 2021). В последние годы в России также был проработан целый ряд вопросов, связанных с регулированием медиапространства, а ценностный суверенитет рассматривается уже как отдельное направление обеспечения национальной безопасности.

В процессе оказания информационных услуг необходим учет рыночным регулятором негативных экстерналий, влияющих на структуру потребительского спроса, политическую систему и принципы целеполагания в стране. Учет законных требований регулятора создаст предпосылки для ухода от неокOLONIALных моделей взаимодействия глобальных ИТ-холдингов с медиасредой западных стран.

²⁹ Журавлева Е. В. Регулирование социальных медиа в КНР // РСМД. 24.01.2022. URL: <https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/regulirovanie-sotsialnykh-media-v-knr/> (дата обращения: 17.02.2022).

³⁰ Курьлев К. П. Регулирование Интернета на постсоветском пространстве // РСМД. 15.11.2021. URL: <https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/regulirovanie-interneta-na-postsovetskom-prostranstve/> (дата обращения: 17.02.2022).

Поступила в редакцию / Received: 20.01.2022
Доработана после рецензирования / Revised: 16.02.2022
Принята к публикации / Accepted: 18.04.2022

Библиографический список

- Агамбен Дж. Номо Сакер. Суверенная власть и голая жизнь. Москва : Европа, 2011.
- Ахмадеев К. Н., Бреслер М. Г., Манойло А. В. Эффективность fake news как инструмента информационной войны в восприятии поколения Z // Вестник Московского государственного областного университета. 2021. № 3. С. 8—32. <https://doi.org/10.18384/2224-0209-2021-3-1084>
- Бегалинова К. К., Грибин Н. П., Комлева В. В., Котюкова Т. В., Назаров Р. Р. и др. Коммуникационные режимы в странах Центральной Азии: научная дискуссия // Россия и мир: научный диалог. 2021. Т. 1, № 2. С. 96—137. <https://doi.org/10.53658/RW2021-1-2-96-137>
- Володенков С. В., Воронов А. С., Леонтьева Л. С., Сухарева М. Цифровой суверенитет современного государства в условиях технологических трансформаций: содержание и особенности // Полилог. 2021. Т. 5, № 1. <https://doi.org/10.18254/S258770110014073-2>

- Гасумянов В. И., Комлева В. В. Коммуникационные режимы как фактор межстрановых взаимодействий: постановка проблемы // *Международная жизнь*. 2020. № 10. С. 38—49.
- Данилин И. В. Влияние цифровых технологий на лидерство в глобальных процессах: от платформ к рынкам? // *Вестник МГИМО-Университета*. 2020. Т. 13, № 1. С. 100—116. <https://doi.org/10.24833/2071-8160-2020-1-70-100-116>
- Дегтерев Д. А. Теоретико-игровой анализ международных отношений. Москва : Аспект Пресс, 2017.
- Дегтерев Д. А. Теоретико-игровой подход в маркетинге. Москва : РУДН, 2014.
- Дегтерев Д. А., Рамич М. С., Пискунов Д. А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // *Вестник международных организаций*. 2021а. Т. 16, № 3. С. 7—33. <https://doi.org/10.17323/1996-7845-2021-03-01>
- Дегтерев Д. А., Рамич М. С., Цвык А. В. США — КНР: «властный транзит» и контуры «конфликтной биполярности» // *Вестник Российского университета дружбы народов. Серия: Международные отношения*. 2021б. Т. 21, № 2. С. 210—231. <https://doi.org/10.22363/2313-0660-2021-21-2-210-231>
- Журавлева Е. В. Китайский опыт продвижения норм и ценностей путем регулирования социальных медиа // *Проблемы Дальнего Востока*. 2022. № 2. С. 97—110. <https://doi.org/10.31857/S013128120019294-4>
- Зиновьева Е. С. Глобальное управление Интернетом: российский подход и международная практика // *Вестник МГИМО-Университета*. 2015. Т. 43, № 4. С. 111—118. <https://doi.org/10.24833/2071-8160-2015-4-43-111-118>
- Зиновьева Е. С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции: дис. ... д-ра полит. наук. Москва : МГИМО, 2019.
- Зиновьева Е. С. Формирование цифровых границ и информационная глобализация: анализ с позиций критической географии // *Полис. Политические исследования*. 2022. № 2. С. 8—21. <https://doi.org/10.17976/jpps/2022.02.02>
- Кутюр С., Тоупин С. Что означает понятие «суверенитет» в цифровом мире? // *Вестник международных организаций*. 2020. Т. 15, № 4. С. 48—69. <https://doi.org/10.17323/1996-7845-2020-04-03>
- Лавлок К. Маркетинг услуг: персонал, технологии, стратегии. 4-е изд. Москва : Вильямс, 2005.
- Лукин А. В. Право на безумие // *Россия в глобальной политике*. 2021. Т. 19, № 5. С. 172—192. <https://doi.org/10.31278/1810-6439-2021-19-5-172-192>
- Манохин В. А. Экстерналии развития информационного рынка: дис. ... канд. эконом. наук. Саратов : СГСЭУ, 2010.
- Международные отношения России в «новых политических пространствах». Космос. Приполярные зоны. Воздушные и морские пространства. Глобальная информационная сфера / под ред. А. Д. Богатурова. Москва : URSS, 2011.
- Нечаев В. Д., Белоконов С. Ю. Цифровая экономика и тенденции политического развития современных обществ // *Контуры глобальных трансформаций: политика, экономика, право*. 2020. Т. 13, № 2. С. 112—133. <https://doi.org/10.23932/2542-0240-2020-13-2-6>
- Понька Т. И., Рамич М. С., У Ю. Информационная политика и информационная безопасность КНР: развитие, подходы и реализация // *Вестник Российского университета дружбы народов. Серия: Международные отношения*. 2020. Т. 20, № 2. С. 382—394. <https://doi.org/10.22363/2313-0660-2020-20-2-382-394>
- Федорченко С. Н. Реконцептуализация наследия В.Л. Цымбургского: политическая легитимация в условиях цифровизации международных отношений // *Журнал политических исследований*. 2021. Т. 5, № 2. С. 66—86. <https://doi.org/10.12737/2587-6295-2021-5-2-66-86>
- Фишер С., Дорнбуш Р., Шмалензи Р. Экономика. Москва : Дело, 1995.
- Шмитт К. Диктатура. От истоков современной идеи суверенитета до пролетарской классовой борьбы. Санкт-Петербург : Наука, 2005.
- Bartelson J. A Genealogy of Sovereignty. Cambridge : Cambridge University Press, 1995.
- Burwell F. G., Propp K. The European Union and the Search for Digital Sovereignty: Building “Fortress Europe” or Preparing for a New World? Washington, D.C. : Atlantic Council Future Europe Initiative, 2020.
- Ciasullo V. M., Troisi O., Cosimato S. How Digital Platforms Can Trigger Cultural Value Co-Creation? – A Proposed Model // *Journal of Service Science and Management*. 2018. No. 11. P. 161—181. <https://doi.org/10.4236/jssm.2018.112013>
- Cuihong Cai. Building a New Digitalised World through Technology Centrism // *Digital Debates: CyFy Journal*. 2020. P. 48—53.
- Culpepper P. D., Thelen K. Are We All Amazon Primed? Consumers and the Politics of Platform Power // *Comparative Political Studies*. 2020. Vol. 53, no. 2. P. 288—318. <https://doi.org/10.1177/0010414019852687>
- Katz E. The Two-Step Flow of Communication: An Up-To-Date Report on an Hypothesis // *The Public Opinion Quarterly*. 1957. Vol. 21, no. 1. P. 61—78. <https://doi.org/10.1086/266687>

- Keohane R. O.* Ironies of Sovereignty: The European Union and the United States // *Journal of Common Market Studies*. 2002. Vol. 40, no. 4. P. 743—765. <https://doi.org/10.1111/1468-5965.00396>
- Krasner S. D.* *Sovereignty: Organized Hypocrisy*. Princeton : Princeton University Press, 1999.
- Lewis J.* Digital Sovereignty in a Time of Conflict // *Digital Debates: CyFy Journal*. 2020. P. 65—74.
- Mearsheimer J.* *The Tragedy of Great Power Politics*. New York, NY : W. W. Norton & Company, 2014.
- Noor E.* Rethinking Decoupling: Interdependence, Dependence, Independence // *Digital Debates: CyFy Journal*. 2020. P. 36—46.
- Pohle J., Thiel T.* Digital Sovereignty // *Internet Policy Review*. 2020. Vol. 9, no. 4. P. 1—19. <https://doi.org/10.14763/2020.4.1532>
- PWC.* *Global Entertainment and Media Outlook, 2020—2024*. PricewaterhouseCoopers Norge, 2020.
- Ray T., Warjri L. B., Jayakumar A., Saran S.* Editors' Note // *Digital Debates: CyFy Journal*. 2020. P. 6—11.
- Roberts H., Cows J., Casolari F., Morley J., Taddeo M., Floridi L.* Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies // *Internet Policy Review*. 2021. Vol. 10, no. 3. P. 1—26. <https://doi.org/10.14763/2021.3.1575>
- Strange S.* *State and Markets*. 2nd edition. London : Continuum, 1994.
- Strange S.* *The Retreat of the State: The Diffusion of Power in the World Economy*. Cambridge : Cambridge University Press, 1996. <https://doi.org/10.1017/CBO9780511559143>
- Strauss W., Howe N.* *The Fourth Turning: An American Prophecy — What the Cycles of History Tell Us About America's Next Rendezvous with Destiny*. New York, NY : Broadway Books, 1997.
- Turow J.* *Media Today. Mass Communication in a Converging World*. 7th edition. London : Routledge, 2020.
- Yeli H.* A Three-Perspective Theory of Cyber Sovereignty // *PRISM*. 2017. Vol. 7, no. 2. P. 109—115.

Сведения об авторе: Дегтерев Денис Андреевич — доктор политических наук, кандидат экономических наук, профессор, заведующий кафедрой теории и истории международных отношений Российского университета дружбы народов; профессор кафедры мировой экономики МГИМО МИД России; профессор кафедры европейских исследований СПбГУ; ORCID: 0000-0001-7426-1383; e-mail: degterev-da@rudn.ru

МЕЖДУНАРОДНЫЕ ЭКОНОМИЧЕСКИЕ ОТНОШЕНИЯ

INTERNATIONAL ECONOMIC RELATIONS

DOI: 10.22363/2313-0660-2022-22-2-372-384

Научная статья / Research article

Цифровой разрыв и цифровое неравенство в продовольственных системах мира

Л.С. Ревенко¹  , Н.С. Ревенко² ¹ МГИМО МИД России, Москва, Российская Федерация² Институт исследований международных экономических отношений

Финансового университета при Правительстве Российской Федерации, Москва, Российская Федерация

 l.revenko@inno.mgimo.ru

Аннотация. Исследуется влияние цифрового разрыва и цифрового неравенства на процессы преобразований в продовольственном секторе мира через призму новой парадигмы, выработанной в период подготовки состоявшегося в сентябре 2021 г. Саммита ООН по продовольственным системам. Целью исследования является выявление основных причин углубления цифрового неравенства в продовольственной сфере и путей его преодоления. Используемая авторами методология междисциплинарного комплексного анализа социально-экономических процессов позволяет выявить места формирования наиболее «разрывных» точек в процессах обеспечения населения мира продовольствием в контексте цифровизации. Обосновывается тезис о том, что в основе проявления цифрового неравенства в различных продовольственных системах лежит разнотемповый характер процессов цифровизации в отдельных странах и среди групп хозяйствующих субъектов, что создает новые условия конкуренции и, соответственно, новое соотношение рыночных преимуществ и рисков. Делается вывод о том, что в продовольственных системах мира цифровое неравенство имеет не только рыночные, но и явно выраженные социальные аспекты, поскольку оно обостряет проблему продовольственной безопасности в части экономической доступности питания из-за снижения или потери доходов сельского населения, теряющего работу в условиях цифровизации, а также порождает новые риски функционирования в цифровых экосистемах. Такая ситуация затрудняет достижение Целей устойчивого развития (ЦУР) до 2030 г., а именно ЦУР-2 и связанных с ней целей. При этом воздействие мер государственного регулирования продовольственного сектора на проблему преодоления цифрового неравенства носит неоднозначный характер.

Ключевые слова: продовольственные системы, продовольственная безопасность, цифровой разрыв, цифровое неравенство

Для цитирования: Ревенко Л. С., Ревенко Н. С. Цифровой разрыв и цифровое неравенство в продовольственных системах мира // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 372—384. <https://doi.org/10.22363/2313-0660-2022-22-2-372-384>

Digital Divide and Digital Inequality in Global Food Systems

Lilia S. Revenko¹  , Nikolay S. Revenko² 

¹MGIMO University, Moscow, Russian Federation

²Financial University under the Government of the Russian Federation, Moscow, Russian Federation

 l.revenko@inno.mgimo.ru

Abstract. The article explores the impact of the digital divide and digital inequality on the transformation processes in the world's food sector through the lens of a new paradigm developed in preparation of the September 2021 UN Food Systems Summit. The purpose of the study is to identify the main causes of the deepening digital inequality in the food sector and ways to overcome it. The authors' methodology of interdisciplinary comprehensive analysis of socio-economic processes makes it possible to identify the most disruptive points that inhibit food provision to the global population in the context of digitalization. It is argued that the digital inequality in various food systems is based on the multi-speed nature of digitalization processes in individual countries and among groups of economic entities, and this creates new competitive landscape and, consequently, a new ratio of market advantages and risks. It is concluded that the digital inequality in the global food systems has implication beyond the market profoundly affecting social outcomes. It exacerbates the food security problem in terms of economic affordability of food due to a decrease or loss of income of the rural population, who lose their jobs in the digitalization context, and also generates new risks of functioning in digital ecosystems. This situation makes it difficult to achieve the 2030 Sustainable Development Goals (SDG), namely SDG-2 and related goals. However, the impact of government regulation of the food sector on overcoming digital inequality remains ambiguous.

Key words: food systems, food security, digital divide, digital inequality

For citation: Revenko, L. S., & Revenko, N. S. Digital divide and digital inequality in global food systems. *Vestnik RUDN. International Relations*, 22(2), 372—384. <https://doi.org/10.22363/2313-0660-2022-22-2-372-384>

Введение

Цифровые технологии (ЦТ), стремительно ворвавшись в экономическую жизнь мира, преобразовывают условия и факторы производственного процесса на всех его стадиях и во всех отраслях. Детально проработанная на макроэкономическом уровне тема их подрывного характера требует анализа в отраслевом, региональном, рыночном и социальном аспектах. Существуют сферы человеческого бытия, где влияние ЦТ проявляется наиболее остро в контексте как получения неоспоримых преимуществ, так и обретения весьма значимых рисков, чреватых угрозой дестабилизации жизни отдельных категорий населения.

Наиболее чувствительной сферой в этой связи можно считать обеспечение населения мира продовольствием. Несмотря на внимание мирового сообщества к вопросу ликвидации

голода, показатели продовольственной безопасности мира ухудшаются. В 2020 г. показатель недоедания в мире вырос с 720 до 811 млн чел., то есть стал на 70—161 млн чел. больше, чем в 2019 г.¹ Одной из причин столь резкого изменения ситуации можно считать пандемию COVID-19, однако она не является единственной.

Комплексный характер причин ухудшения состояния продовольственной безопасности и, как следствие, невозможность достижения ЦУР-2 Целей устойчивого развития (ЦУР) стали причиной созыва в сентябре 2021 г. Саммита ООН по продовольственным

¹ The State of Food Security and Nutrition in the World 2021. Transforming Food Systems for Food Security, Improved Nutrition and Affordable Healthy Diets for All. Rome: FAO, 2021. P. 8, 11, 15. URL: <https://www.fao.org/3/cb4474en/cb4474en.pdf> (accessed: 28.12.2021).

системам (ПС), на котором были сформулированы новые подходы к их трансформации. Совокупность предложенных концепций легла в основу современной парадигмы ПС (Ревенко, Солдатенкова, Ревенко, 2021, с. 99). При множестве взглядов на эту проблему прослеживается необходимость опоры в трансформации ПС на инновации и их инклюзивное применение.

Совершенствование ПС с учетом использования инновационных решений в производстве, распределении и потреблении продовольствия предполагает учет неравных технологических возможностей и рисков для разных категорий хозяйствующих субъектов и физических лиц. По некоторым оценкам, в производстве и распределении продовольствия прямо или косвенно занято 4 млрд чел.² Соответственно, баланс преимуществ и рисков от использования ЦТ имеет не только экономический, но и социальный контекст для тех, кто создает продовольствие и для тех, кто его потребляет.

Целью данного исследования является выявление основных причин формирования цифрового разрыва и цифрового неравенства в продовольственной сфере, а также поиск путей их преодоления.

Обзор литературы и методология

Методологические подходы к рассмотрению поставленной цели основаны на принципах междисциплинарности, поскольку в данной тематике сходятся технологические, экономические, экологические, социальные аспекты. Основой примененной методологии исследования можно считать комплексный подход к анализу социально-экономической системы, включающий в себя применение методов исследования трендов, сопоставления и систематизации, исторической компаративистики.

² Положение дел в области продовольствия и сельского хозяйства: преобразование агропродовольственных систем: от стратегий к действиям. Конференция, сорок вторая сессия, 2021 год // Продовольственная и сельскохозяйственная организация Объединенных Наций. URL: <https://www.fao.org/3/nf243ru/nf243ru.pdf> (дата обращения: 06.01.2022).

В теоретическом плане исследование опирается на труды зарубежных и российских ученых в области проблем цифровизации в ПС. Так, группа британских исследователей (Brewer et al., 2021) полагает, что преобразованный в цифровую форму потенциал продовольственной системы может быть реализован, только если данные будут беспрепятственно проходить по всей цепи поставок от производителей к потребителям. Влияние экологических проблем и неравенства в питании в странах мира, оказываемое сегодня на продовольственную систему, рассмотрено М.Е. Брассеско, М. Пинтадо и Е.Р. Коскуетой (Brassesco, Pintado & Coscueta, 2022). По их мнению, для восстановления этой системы необходимы перестройка производственно-сбытовых цепочек и внедрение цифровых технологий.

М.В. Шатилов, Р.А. Мещерякова и М.И. Иванова (2021) приводят пример внедрения цифровых площадок и продуктов, снижающих издержки производителей сельскохозяйственной продукции и повышающих эффективность деятельности участников этого рынка. Анализ основных информационных систем АПК в контексте управления системой обеспечения продовольствием и перспективных направлений развития цифровизации сельскохозяйственного сектора осуществлен в исследованиях В.И. Харитоновой (2021a; 2021b). Ключевые факторы, препятствующие цифровизации агропромышленного комплекса, выявлены Т.П. Максимовой и О.А. Ждановой (2018).

Из немногочисленных исследований влияния цифрового неравенства и цифрового разрыва в продовольственных системах следует выделить работу К. Бронсон и И. Кнезевич, в которой акцентируется неравенство в доступе к большим данным со стороны фермеров и крупных представителей агробизнеса Канады (Bronson & Knezevic, 2019). Эта же проблема проанализирована А. Веерсинком, Е. Фрезером, Д. Паннеллом, Э. Данкан и С. Ротц (Weersink et al., 2018). Вопрос формирования устойчивых и неустойчивых методов производства посредством цифровых технологий рассмотрен в исследовании

С.Л.Р. Крука, С. Клоппенбург, Х.М. Тоонен и С. Буша (Kruk et al., 2021). В этом труде также делается акцент на процессах преодоления существующих барьеров роста производства с помощью цифровых технологий либо выстраивания новых процессов.

Анализ научных трудов позволил выделить максимально широкий спектр дискуссий по тематике цифрового разрыва. В исследованиях Я. ван Дайка объяснены причины расширения и углубления цифрового разрыва, показано, что он заключается не только в доступе к Интернету, но и возможности профессионально использовать новые средства массовой информации или создавать новую культуру (Van Dijk, 2005; 2012). Им также выделены три уровня цифрового разрыва: физический доступ к Интернету, цифровые навыки пользователей и новый — социальные преимущества, получаемые пользователями при грамотном использовании информационно-коммуникационных технологий (ИКТ), названный им результатами цифрового разрыва. Последний уровень, по его мнению, с одной стороны, создает дополнительный потенциал, например, в социальной и политической сферах, а с другой — порождает отрицательные эффекты (понижение уровня безопасности, киберпреступность и др.) (Van Dijk, 2020). Три уровня цифрового неравенства в России изучены также в работе А.А. Гладковой, З.Г. Гарифуллина и М. Рагнедды (2019), а вопрос о роли третьего уровня в контексте определения субъектов — основных получателей выгод от онлайн-доступа — в исследовании А. ван Дёрсена и Э.Й. Хелспер (Van Deursen & Helsper, 2015).

Проблема цифрового разрыва через призму доступа к Интернету и социального неравенства проанализирована М. Рагнеддой и Г. Мушерттом (Ragnedda & Muschert, 2013). Е. Харгиттай исследовал проблему неравенства физических лиц в доступе к Интернету и в привлечении производителями контента пользователей к своим онлайн-материалам (Hargittai, 2003). Под углом неравных условий доступа к Интернету проблема цифрового неравенства изучена Б. Райсдорф, У. Даттоном, В. Тривибово и М. Нелсоном (Reisdorf et al., 2017).

Цифровой разрыв в контексте социокультурных изменений и динамики принятия решений по вопросу внедрения ИКТ в качественном и количественном выражениях проанализирован в работе П. Цацу, где предлагается рассматривать цифровой разрыв в сложном контексте, когда лица, принимающие решения и решающие проблемы, взаимодействуют с обычными людьми и их культурами (Tsatsou, 2011).

Уточняющая современная трактовка цифрового разрыва содержится в актуальном Докладе ЮНКТАД о цифровой экономике 2021, где отмечается, что традиционное его понимание как возможность подключения и доступа к Интернету необходимо дополнять его новыми измерениями, связанными с «цепочкой создания стоимости данных»³.

Проблемы, которые вследствие цифрового неравенства препятствуют социальному, экономическому и политическому прогрессу в Африке, рассмотрены в исследовании Б. Муцвайро и М. Рагнедды (Mutsvairo & Ragnedda, 2019).

Важными представляются также исследования темы формирования цифрового капитала при расширении цифрового разрыва. Так, С. Парк ввела понятие цифрового капитала, относящееся к условиям, определяющим доступ, использование и взаимодействие людей с цифровыми технологиями, и провела анализ того, как возникают новые формы цифрового неравенства в зависимости от цифровой экосистемы пользователя (Park, 2017).

М. Рагнедда, основываясь на работах П. Бурдьё, в которых было введено понятие «информационного капитала», сформулировал определение цифрового капитала. Им, полагает он, является «накопление цифровых компетенций (информационных, коммуникационных, безопасных, создающих контент и решающих проблемы) и цифровых технологий» (Ragnedda, 2018, p. 2367). При этом

³ Доклад о цифровой экономике 2021: Международные потоки данных и развитие: кому служат потоки данных. Женева: ЮНКТАД, 2021. С. 3. URL: https://unctad.org/system/files/official-document/der2021_overview_ru.pdf (дата обращения: 08.05.2022).

уровень цифрового капитала пользователя влияет на качество работы в Интернете, которое, в свою очередь, может быть преобразовано в экономическую, культурную, социальную, политическую и другие формы капитала. Концептуальные вопросы и основы теории цифрового капитала рассмотрены также в работах М. Рагнеллы, М.Л. Руиу (Ragnedda & Ruiu, 2020), Е.Л. Вартановой и А.А. Гладковой (2021).

В данном исследовании авторы также принимали во внимание реализацию в России федерального проекта «Устранение цифрового неравенства»⁴ и аналогичные проекты цифровой экономики других стран, в частности «Цифровая Индия»⁵.

Следует отметить, что понятия «цифровой разрыв» и «цифровое неравенство» достаточно близки, но между ними есть и некоторые различия. Хотя устоявшегося официального определения цифрового разрыва нет, по мнению авторов, наиболее правильно его суть сформулирована экспертами ОЭСР: это «разрыв между отдельными лицами, домашними хозяйствами, предприятиями и географическими районами на разных социально-экономических уровнях с точки зрения как экономических уровней, так и их возможностей доступа к ИКТ и использования Интернета для широкого спектра видов деятельности»⁶. Также отсутствует общепризнанное определение термина «цифровое неравенство». Под ним авторы данной статьи понимают неравноценное получение экономических и социальных благ по причине невозможности адекватного использования достижений цифровых технологий. В ряде случаев, однако, понятия становятся синонимичными,

⁴ Программа устранения цифрового неравенства в России // TAdviser. 20.12.2021. URL: https://www.tadviser.ru/index.php/Статья:Программа_по_устранению_цифрового_неравенства_в_России (дата обращения: 08.05.2022).

⁵ Digital India// Ministry of Electronics & Information Technology of India. URL: <https://www.digitalindia.gov.in> (accessed: 08.05.2022).

⁶ How to Measure the Digital Divide? // Korea Agency for Digital Opportunities & Promotion. URL: <https://www.itu.int/osg/spu/ni/digitalbridges/presentations/02-Cho-Background.pdf> (accessed: 08.03.2022).

что отражает реально сложившуюся ситуацию в экономике и научном дискурсе.

При проведении данного исследования авторы опираются на дефиниции и индикаторы, выработанные преимущественно в международных организациях системы ООН. Так, базовое определение ПС, выработанное в ООН, характеризует их как «весь спектр действующих лиц, видов деятельности и биофизической и социально-экономической среды, участвующих в производстве, переработке, распределении, регулировании и потреблении пищевых продуктов»⁷. Инклюзивность ПС трактуется как их свойство, предполагающее обеспечение доступа всех людей, особенно лиц и общественных групп, находящихся в социально и экономически неблагоприятном положении, к недорогим, безопасным и питательным продуктам питания, а также предоставление возможности каждому справедливо пользоваться своими экономическими выгодами⁸. В статье сквозь призму этих дефиниций рассматривается проблематика цифрового разрыва и неравенства в ПС.

Специфика цифрового разрыва в продовольственных системах

В ПС мира цифровой разрыв проявляется во множественных формах и видах. Степень его проявления зависит от уровня развития страны, типа производственных систем, характера инновационной экосистемы, образовательного уровня населения, доходов, демографической структуры и других условий функционирования ПС.

В современной парадигме развития ПС инновационная компонента является доминирующей в контексте повышения эффективности производственных процессов, снижения

⁷ Policy Brief: The Impact of COVID-19 on Food Security and Nutrition // UN Sustainable Development Group. June 2020. P. 2. URL: <https://unsdg.un.org/sites/default/files/2020-06/SG-Policy-Brief-on-COVID-Impact-on-Food-Security.pdf> (accessed: 24.12.2021).

⁸ Global Food Policy Report: Building Inclusive Food Systems // International Food Policy Research Institute (IFPRI). 2020. P. 9, 11. URL: <https://ebrary.ifpri.org/utils/getfile/collection/p15738coll2/id/133646/filename/133857.pdf> (accessed: 25.12.2021).

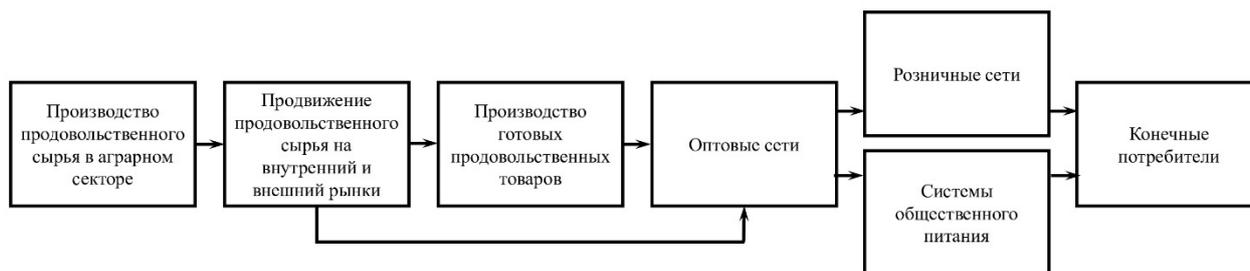


Рис. 1. Производственно-сбытовая цепь в продовольственном секторе

Источник: составлено авторами.

голода и недоедания, а также решения экологических задач. Как и в других отраслях, ускорение научно-технического прогресса (НТП) в ПС влечет за собой технологические разрывы, в том числе цифровой. Многие исследователи сходятся во мнении, что в целом в экономике «ускорение темпов современной цифровизации усугубляет проблему цифрового неравенства» (Сафиуллин, Моисеева, 2019, с. 27).

Для России эта проблема также чрезвычайно актуальна, и она заслуживает отдельного детализированного анализа, который присутствует в научной среде. Кроме научных исследований этой тематике посвящены обзоры консультационных компаний и официальных структур (Архипов и др., 2019).

В силу особенностей воспроизводственного процесса в ПС для целей данного исследования важно выделить элементы продовольственной цепи. Представленная на рис. 1 схема показывает продвижение продовольствия «от поля до тарелки».

Участие в глобальных производственно-сбытовых цепочках (ГПСЦ) дает неоспоримые конкурентные преимущества участникам рынка. Возможности встраивания в ГПСЦ во многом зависят от потенциала и практики использования ЦТ субъектами ПС. На глобальном уровне именно в этой сфере проявляется цифровое неравенство как невозможность для многих хозяйствующих субъектов быть встроенными в процессы глобального обмена.

При том, что противоречия цифровой эпохи в мировой ПС наиболее явно проявляются в сфере обмена, вызревают они (и во многом уже сформированы) на стадии производства. Поэтому есть необходимость

выделить основные виды цифрового разрыва и неравенства в отдельных звеньях цепи (табл. 1).

Первым звеном в производственной цепи продовольственного сектора является сырьевой, то есть сфера создания продукции растениеводства, животноводства, рыбного хозяйства. Поскольку особенностью данной сферы является тесная связь с социальной жизнью населения, производящего такую продукцию, процессы цифровизации здесь особо ярко проявляют свой дуализм, единство преимуществ и рисков. Именно поэтому авторы сосредоточились в работе на данном звене создания продовольствия.

Цифровой разрыв в сырьевом секторе продовольственных систем

Для оценки уровня цифровизации существует ряд разработанных универсальных для всех отраслей показателей. Базовым показателем цифрового разрыва, как следует из проведенного анализа научных трудов предшественников и данных международных организаций, можно считать доступ к Интернету для городского и сельского населения (табл. 2).

Согласно этим индикаторам, сельское население имеет меньший доступ к ЦТ. Для сельских территорий характерны нехватка инфраструктуры, неэффективность институтов, ответственных за внедрение ЦТ, отсутствие или ограниченный доступ к цифровым услугам. Кроме того, по всем показателям, за исключением охвата городского населения мобильной связью 2G, существует большая дисперсия между странами с разным уровнем

Таблица 1

Типология цифрового неравенства в продовольственных системах

Основные звенья продовольственной цепи	Виды цифрового неравенства
Производство продовольственного сырья в аграрном секторе	<ul style="list-style-type: none"> — По доступу к информации о ресурсах, условиях функционирования — По доступу к цифровым геопространственным, рыночным, бытовым, обучающим платформам — По возможностям использования Интернета вещей, технологий точного земледелия и умного животноводства — По способам формирования новых организационных форм ведения бизнеса
Производство готовой продукции в пищевых отраслях	<ul style="list-style-type: none"> — По уровню автоматизации и роботизации основных и вспомогательных производственных процессов — По возможностям использования Интернета вещей — По способности регулировать квалификационную структуру и количество привлекаемого персонала — По оптимизации затрат на единицу продукции
Товародвижение и реализация сырьевой и готовой пищевой продукции	<ul style="list-style-type: none"> — По доступу к сбытовой инфраструктуре — По возможности быть «видимым» для контрагентов — По способности поставлять продукцию в оптимальном объеме в места формирования спроса — По способности осуществлять мониторинг рынка — По возможности отслеживать цены на свою продукцию и на требуемые ресурсы

Источник: составлено авторами.

Таблица 2

Основные показатели цифровизации города и села, %

Показатель	2015		2020		2021*	
	В городах	В сельской местности	В городах	В сельской местности	В городах	В сельской местности
Обеспеченность населения мобильной связью не менее LTE/WiMAX						
В среднем в мире	64,1	19,3	95,3	71,7	97,0	75,4
В развитых странах	92,3	60,6	100,0	88,9	100,0	93,4
В развивающихся странах	54,8	15,7	93,9	70,2	96,1	73,8
В наименее развитых странах	31,2	7,9	73,4	28,6	89,0	33,6
Процент лиц, использующих Интернет						
В среднем в мире	н/д	н/д	75,6	38,8	н/д	н/д
В развитых странах	н/д	н/д	89,4	85,1	н/д	н/д
В развивающихся странах	н/д	н/д	71,7	33,8	н/д	н/д
В наименее развитых странах	н/д	н/д	47,1	12,9	н/д	н/д

Примечания: * оценочные данные; н/д — нет данных.

Источник: Key ICT indicators by urban/rural area (penetration rates) // International Telecommunication Union. URL: <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx> (accessed: 10.01.2022).

развития. Вместе с тем прогнозируется увеличение объема производства сельскохозяйственной продукции в мире на 500 млн т и сокращение потерь на 65 млн т к 2030 г. только за счет использования технологий мобильной связи⁹. При том, что для обеспечения

⁹ Байты и продовольствие: применение цифровых технологий в сельском хозяйстве для достижения целей в области устойчивого развития (ЦУР).

относительно равных возможностей субъектам ПС требуется не только доступ, но и контент, все же подключение к сети лежит в основе преодоления цифрового разрыва в этой сфере.

Региональная конференция ФАО для Азии и Тихого океана, 1—4 сентября 2020 года // Продовольственная и сельскохозяйственная организация Объединенных Наций. URL: <https://www.fao.org/3/nb844ru/NB844RU.pdf> (дата обращения: 21.12.2021).

По мнению экспертов ФАО и других международных организаций, растущий цифровой разрыв может стать «новым лицом неравенства», поскольку отсутствие доступа делает автономными почти половину населения планеты¹⁰. Весьма эмоционально, но точно высказался по этому поводу представитель аграрного сообщества Бангладеш А. Борхан на заседании Региональной конференции Продовольственной и сельскохозяйственной организации ООН (ФАО) для Азии и Тихого океана: «Нам нужна не просто цифровизация — нам также нужна цифровая справедливость», под которой мелкие земледельцы Азии понимают самые элементарные технологии, обеспечивающие связь с внешней средой для получения базовой информации о погоде, рынках, доступу к образованию¹¹.

Вопрос подключения сельских территорий к Интернету лежит в основе цифровой интеграции как явления, противоположного цифровому неравенству и означающему сглаживание разрыва в хозяйственных и социальных возможностях отдельных субъектов. В ПС цифровая интеграция означает также и улучшение физического и экономического доступа к продовольствию. К этому блоку проблем цифровизации в продовольственном секторе проявляется особое внимание в международных организациях. Так, в ФАО обозначают необходимость обеспечения цифровой интеграции через ликвидацию цифрового разрыва в ПС в общемировом масштабе для устранения диспропорций продовольственных рынков, асимметрии информации о ценах на готовую продукцию и ресурсы всех видов, а также для обеспечения доступа к финансовым услугам и

государственной поддержке. Подчеркивается опасность «цифровой пропасти» между городским и сельским населением, а также гендерный аспект цифрового неравенства. Опираясь на информацию Комиссии по широкополосной связи о том, что для подключения всех индивидуумов к Интернету до 2030 г. потребуются инвестиции в 428 млрд долл. США¹², в ФАО делают вывод о сопоставимости этих инвестиций с издержками от цифрового разрыва.

Нельзя не учитывать и исторический контекст цифрового неравенства в процессе эволюции ПС. Существует подход к анализу причин цифрового неравенства через призму традиционно складывающихся земельных отношений. В исследовании, проведенном аналитическим центром Research ICT Africa, проводится мысль о том, что результатом исторического развития в ЮАР явилось расслоение земельного ресурса между крупными высокоэффективными землевладельцами колониальной эпохи, имеющими возможность за счет эффекта масштаба пользоваться инфраструктурой, банковскими и страховыми продуктами, и мелкими хозяйствами коренного населения, которые такой возможности лишены. Соответственно крупные и мелкие хозяйства имеют разный доступ к цифровым технологиям в силу масштаба деятельности, определяемому размером обрабатываемой земли¹³.

В силу высоких затрат современные ЦТ применяются только в крупномасштабных хозяйствах ЮАР. В небольших хозяйствах выгоды от использования цифровых технологий извлекаются лишь из примитивных приложений, таких как системы распространения сельскохозяйственной и рыночной

¹⁰ The Digital Divide Risks Becoming the “New Face of Inequality” // FAO Liaison Office in New York. April 27, 2021. URL: <https://www.fao.org/new-york/news/detail/es/c/1397201/> (accessed: 08.03.2022).

¹¹ Заявление представителя консультативного совещания с гражданским обществом. Региональная конференция ФАО для Азии и Тихого океана, 8—11 марта 2022 г. // Продовольственная и сельскохозяйственная организация Объединенных Наций. URL: <https://www.fao.org/3/ni500ru/ni500ru.pdf> (дата обращения: 08.04.2022).

¹² G20: FAO DG Calls for Closing of Digital Divide in Agriculture // AgriculturePost. August 5, 2021. URL: <https://agriculturepost.com/g20-fao-dg-calls-for-closing-of-digital-divide-in-agriculture/> (accessed: 28.12.2021).

¹³ Aguera P., Berglund N., Chinembiri T., Comminos A., Gillwald A., Govan-Vassen N. Paving the Way Towards Digitalising Agriculture in South Africa. Cape Town: Research ICT Africa, 2020. P. 12—13. URL: <https://researchictafrica.net/wp/wp-content/uploads/2020/09/PavingthewaytowardsdigitalisingagricultureinSouthAfricaWhitepaper272020105251.pdf> (accessed: 28.12.2021).

информации, доступные с помощью мобильных устройств.

Связь цифрового неравенства с геопространственными факторами подчеркивается и в работах других исследователей. Так, Дж.Т. Бартелс и М. Беннис, анализируя причины цифрового неравенства на Аляске, не ограничиваются его чисто технологическими аспектами. Они отмечают сочетание открытых ландшафтов и наличие небольших поселений коренного населения преимущественно вдоль береговых линий в качестве препятствия экономического характера, когда развитие цифровой инфраструктуры технически возможно, но экономически невыгодно (Bartels & Bennice, 2020). Проблемам технологических разрывов в рассматриваемой сфере посвящено также развернутое исследование под редакцией Ф.В. Гатцвайлера и Й. фон Брауна (Gatzweiler & von Braun, 2016).

Оценка общего уровня цифрового неравенства осуществляется с использованием показателей доступности ЦТ. Например, по России она проведена в работе М.Ю. Архиповой, В.П. Сиротина и Н.А. Сухаревой (2018). Региональные аспекты цифрового разрыва в странах БРИКС рассматриваются в работе А.К. Морозкиной (2020).

Преодоление цифрового разрыва является одним из приоритетов в процессе мер, принимаемых многими странами в целях успешного решения проблемы продовольственного обеспечения через трансформацию ПС. Поощряются формы государственно-частного партнерства для постоянного и надежного подключения к Интернету в сельских районах, расширения охвата мобильной сетью 3G и 4G для работы с поставщиками услуг, функционирования Интернета вещей. Важным направлением является повышение цифровой грамотности фермеров. Однако для ряда регионов стоит более скромная задача: предоставление фермерам экономической возможности пользоваться смартфонами и обучение применению базовых приложений для этих устройств.

Смартфоны во многих сельских сообществах мира являются единственным оборудованием, позволяющим пользоваться профессиональной информацией через платформы,

приложения, а также участвовать в процессе реализации своих товаров в новых условиях конкуренции. Влияние смартфонов на функционирование ПС в различных регионах мира исследуется с экономической и социальной точек зрения. Так, Д. Прабха и Р. Аруначалам на основе эмпирических исследований в регионах Индии пришли к выводу, что эти устройства в значительной степени помогли фермерам улучшить доступ к государственным консультационным услугам. Это повлияло на технологическое оснащение ферм, социальный климат, но заметно не затронуло экономическую составляющую производственного процесса (Prabha & Arunachalam, 2019).

Интересен рассмотренный в исследовании Х. Баумюллер (Baumüller, 2016) опыт формирования местной инновационной среды, изначально опирающейся на использование смартфонов, в Кении. За счет поддержки этого сектора правительством Кения стала лидером в области ЦТ в странах Африки к югу от Сахары.

Поиск путей ликвидации цифрового неравенства является целью многих научных исследований. Например, в работе по цифровизации регионов Индии (Uradhyaya et al., 2019) в качестве подлежащих устранению причин неравенства выделяются дифференцированный доступ к инструментам ЦТ, низкая цифровая грамотность, не всегда подходящий для фермеров контент, отсутствие устойчивого Интернета и даже электричества. В другой работе этих авторов делается вывод, что эффективность ЦТ в разных регионах Индии зависит не только от их доступности, но и от возраста, пола пользователя, уровня его осведомленности о возможностях, а также от участия в жизни общины (Uradhyaya et al., 2018).

Проблема цифровой интеграции актуальна не только для развивающихся стран. В Канаде прилагаются усилия для реализации программ цифрового развития коренных народов и маргинализированных сообществ. Одновременно ведутся дискуссии о влиянии аграрных ЦТ на рынок труда, а именно на занятость и уровень доходов сельскохозяйственных

работников. Рабочие места в сырьевом секторе ПС далеко не всегда могут быть заполнены претендентами из-за несоответствия их навыков и умения использовать ЦТ. Трудно не согласиться с мнением канадских исследователей, что цифровое неравенство может не только фиксировать, но и усиливать социальное неравенство в рассматриваемой сфере (Rotz et al., 2019, pp. 113, 115). То же самое можно констатировать применительно к использованию больших данных (Carolan, 2018, p. 171).

Невозможность доступа к Интернету полностью блокирует использование в сырьевом продовольственном секторе таких современных технологий, как Интернет вещей, прецизионное земледелие, «умное» животноводство, робототехника, получение информации, встраивание в производственно-сбытовые цепочки с использованием цифровых платформ и др. Элементы такого сценария развития были обозначены еще в предыдущем десятилетии в работе исследователей из Австралии и Нидерландов (McBratney et al., 2005). Такие технологические решения доступны субъектам, во-первых, встроенным в максимально инновационные цифровые экосистемы, во-вторых, характеризующимся высокой эффективностью и доходностью, которая позволяет им обновлять активную часть основного капитала по высокотехнологичной схеме. С. Сантос Вале и Й. Кинзле систематизировали перечень задач растениеводства, которые современные роботы могут выполнять самостоятельно под наблюдением человека¹⁴, что в значительной степени меняет структуру затрат и условия конкуренции.

Несмотря на все нюансы цифрового разрыва, однозначным подходом к цифровизации в сырьевом аграрном секторе является ее трактовка как «эффективного пути роста производительности, улучшения качества продукции, оптимизации использования всех

видов ресурсов, повышения благосостояния жителей сельских регионов, улучшения бизнес-процессов на всех этапах создания и продвижения продукции» (Современные проблемы менеджмента..., 2018, с. 519—528).

Риски и вызовы цифрового разрыва в продовольственной сфере

В ПС технологические трансформации несут не только положительные эффекты, но и риски, связанные с цифровым неравенством. В научной литературе их прежде всего связывают с изменением характера занятости. «Риск автоматизации», то есть высвобождения рабочих мест за счет применения ЦТ и соответствующего оборудования, имеет наибольшее значение для тех сфер, где высока доля рутинных работ (Саскинд, 2021, с. 136). Сформировалась так называемая «цифровая ловушка», когда несоответствие навыков для выполнения работы усиливается привязанностью к месту проживания и социуму.

Безусловно, тема минимизации использования человеческого труда в регионах с обширным земельным ресурсом и низкой плотностью населения не носит деструктивного характера. Напротив, этот вектор формирует явно выраженные преимущества. При том, что тема технологической безработицы не нова для экономики мира, в современных условиях функционирования ПС и необходимости решения проблемы голода на планете она приобрела новое значение.

Еще одна группа рисков представлена проблемой безопасности людей в ходе производственных процессов — применения беспилотной техники и роботов на полях, автоматизированных и роботизированных процессов на «умных» фермах и перерабатывающих предприятиях. Необходимость опережающего принятия правил регулирования таких производственных процессов очевидна, но все же между их разработкой и имплементацией существует временной лаг, что создает напряженность между хозяйствующими субъектами и социумом.

Не менее важным аспектом цифрового неравенства в ПС можно считать получение

¹⁴ Santos Valle S., Kienzle J. Agriculture 4.0: Agricultural Robotics and Automated Equipment for Sustainable Crop Production // Integrated Crop Management. Vol. 24. Rome: FAO, 2020. P. 7. URL: <https://www.fao.org/3/cb2186en/CB2186EN.pdf> (accessed: 04.04.2022).

информации о качестве продуктов и безопасности питания, к которой отдельные социальные группы имеют ограниченный доступ. В исследовании о взаимосвязи между инцидентами, связанными с безопасностью пищевых продуктов, и цифровым разрывом делается вывод об усугубляющемся неравенстве в области предотвращения пищевых рисков среди населения, имеющего разный доступ к Интернету (Chiu & Li, 2021).

Нельзя не отметить также риски размытия традиционных схем потребления продовольствия, ликвидации местных промыслов и производств. Привлекательные для одних субъектов схемы встраивания в цепочки создания продуктов, например, через цифровые платформы (Ревенко, 2021, с. 214), на глобальном и национальном уровнях могут лишить целые группы мелких предпринимателей перспектив ведения бизнеса в продовольственной сфере.

Проблемы цифрового неравенства в ПС обострились в условиях пандемии, а ее двойное воздействие по-разному проявляется в отдельных сферах. Если в целом в обществе, особенно в городской среде, можно наблюдать, с одной стороны, осложнение функционирования людей без цифровых навыков, а с другой — их стремление расширить свою цифровую грамотность (Торопова, Соколова, Гусейнов, 2020, с. 459—460), то в ПС этот процесс не протекает так линейно из-за специфики аграрной сферы. Поскольку цифровые экосистемы городского и сельского типов показывают разный уровень развития, а урбанизация и глобализация усиливают отток сельского населения, обладающего цифровой грамотностью, в другие сферы, усиливаются и риски углубления неравенства в доступе к выгодам цифровизации¹⁵.

Снижение физической мобильности фермеров и представителей мелкого продовольственного бизнеса во время пандемии явилось разрушительным для тех из них, кто не опирался на ЦТ в поиске рынков сбыта и в

процессе приобретения ресурсов. Одновременно происходит стимулирование к более широкому использованию ЦТ для обеспечения стабильности бизнеса в продовольственной сфере.

Заключение

Основополагающей причиной цифрового неравенства можно считать уровень экономического развития стран, из которого вытекают социальные, технологические и другие проблемы во всем их спектре — от уровня грамотности до готовности к преобразованиям на ментальном уровне. В контексте цифрового неравенства ПС концептуальное значение имеют разные стартовые условия цифровой трансформации и способность стран экономически обеспечить цифровой рывок или эволюцию системы. Таким образом, в основе проявления цифрового неравенства в ПС лежит разноскоростной характер процессов цифровизации в отдельных странах и компаниях, которые вынуждены функционировать в новой конкурентной среде.

Цифровой разрыв в ПС мира во втором десятилетии XXI в. закрепил ранее сформированные различия в конкурентных условиях функционирования хозяйствующих субъектов. При этом доступ к продовольствию отдельных слоев населения стал все больше зависеть не только от доходов, но и от цифровой грамотности, а также способности воспользоваться преимуществами соответствующих технологий, что особо ярко проявилось в условиях пандемии. Это свидетельствует о явно выраженном социальном аспекте цифрового неравенства в ПС и предполагает усиление регуляторной функции государств для решения проблемы продовольственной безопасности в контексте экономической доступности питания из-за снижения или потери доходов сельского населения, теряющего работу в условиях цифровизации.

Авторы разделяют подход к необходимости преодоления цифрового неравенства в контексте преобразования продовольственной сферы мира в целом и ее отдельных элементов как к системной проблеме, без решения которой невозможно достижение глобальных целей, среди которых обеспече-

¹⁵ Trendov N. M., Varas S., Zeng M. Digital Technologies in Agriculture and Rural Areas: Status Report // FAO. Rome: FAO, 2019. P. 2. URL: <https://www.fao.org/3/ca4985en/ca4985en.pdf> (accessed: 13.01.2022).

ние продовольственной безопасности, повышение инновационного уровня ПС, создание современной инфраструктуры, поддержание биоразнообразия и почвенного плодородия,

сохранение традиционных сельских сообществ, встраивание в рыночную систему производителей и потребителей продовольствия с разными возможностями.

Поступила в редакцию / Received: 19.01.2022
Доработана после рецензирования / Revised: 01.04.2022
Принята к публикации / Accepted: 18.04.2022

Библиографический список

- Архипов А. Г., Косогор С. Н., Моторин О. А., Горбачев М. И., Суворов Г. А., Труфляк Е. В. Цифровая трансформация сельского хозяйства России. Москва : ФГБНУ «Росинформагротех», 2019.
- Архипова М. Ю., Сиротин В. П., Сухарева Н. А. Разработка композитного индикатора для измерения величины и динамики цифрового неравенства в России // Вопросы статистики. 2018. Т. 25, № 4. С. 75—87.
- Вартанова Е. Л., Гладкова А. А. Цифровое неравенство, цифровой капитал, цифровая включенность: динамика теоретических подходов и политических решений // Вестник Московского университета. Серия 10: Журналистика. 2021. № 1. С. 3—29. <https://doi.org/10.30547/vestnik.journ.1.2021.329>
- Гладкова А. А., Гарифуллин В. З., Рагнедда М. Модель трех уровней цифрового неравенства: современные возможности и ограничения (на примере исследования Республики Татарстан) // Вестник Московского университета. Серия 10: Журналистика. 2019. № 4. С. 41—72. <https://doi.org/10.30547/vestnik.journ.4.2019.4172>
- Максимова Т. П., Жданова О. А. Реализация стратегии цифровизации агропромышленного комплекса России: возможности и ограничения // Теория и практика общественного развития. 2018. № 9. С. 63—67. <https://doi.org/10.24158/tipor.2018.9.9>
- Морозкина А. К. Цифровой разрыв в странах БРИКС: проблемы межрегионального неравенства // Вестник международных организаций. 2020. Т. 15, № 4. С. 70—90. <https://doi.org/10.17323/1996-7845-2020-04-04>
- Ревенко Л. С. Мировая продовольственная система: цифровые аспекты трансформации // Научные труды ВЭО России. 2021. Т. 230. С. 213—218. <https://doi.org/10.38197/2072-2060-2021-230-4-217-222>
- Ревенко Л. С., Солдатенкова О. И., Ревенко Н. С. Новая парадигма продовольственных систем // Горизонты экономики. 2021. № 5. С. 99—106.
- Саскинд Д. Технология, автоматизация и стоит ли их бояться. Москва : Индивидуум, 2021.
- Сафиуллин А. Р., Моисеева О. А. Цифровое неравенство: Россия и страны мира в условиях четвертой промышленной революции // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Серия: Экономические науки. 2019. Т. 12, № 6. С. 26—37. <https://doi.org/10.18721/JE.12602>
- Современные проблемы менеджмента, маркетинга и предпринимательства* / под общ. ред. Н.Ю. Кониной. Москва : МГИМО-Университет, 2018.
- Торопова Н. В., Соколова Е. С., Гусейнов Ш. Г. Тенденции цифрового неравенства в цифровой экономике: особенности международной дискриминации // Экономика: вчера, сегодня, завтра. 2020. Т. 10, № 8А. С. 456—463.
- Харитонов В. И. Инструменты формирования цифрового сельского хозяйства в контексте развития системы управления продовольственным обеспечением // E-Scio. 2021a. № 9. С. 262—268.
- Харитонов В. И. Развитие системы продовольственного обеспечения в контексте формирования информационных систем в агропромышленном комплексе // Современная экономика: проблемы и решения. 2021b. № 12. С. 177—190. <https://doi.org/10.17308/meps.2021.12/2741>
- Шамилов М. В., Мецзякова Р. А., Иванова М. И. Трансформация продовольственной системы в условиях цифровизации АПК // Экономика сельского хозяйства России. 2021. № 1. С. 52—60. <https://doi.org/10.32651/211-52>
- Bartels J. T., Bennice M. Digital Inequities in Rural Alaska // *Critical Mobile Pedagogy* / ed. by J. Traxler, H. Crompton. New York : Routledge, 2020. P. 50—63. <https://doi.org/10.4324/9780429261572-4>
- Baumüller H. Agricultural Service Delivery through Mobile Phones: Local Innovation and Technological Opportunities in Kenya // *Technological and Institutional Innovations for Marginalized Smallholders in Agricultural Development* / ed. by F. W. Gatzweiler, J. von Braun. Cham : Springer, 2016. P. 143—159. https://doi.org/10.1007/978-3-319-25718-1_9
- Brassesco M. E., Pintado M., Coscueta E. R. Food System Resilience Thinking: From Digital to Integral // *Science of Food and Agriculture*. 2022. No. 102. P. 887—891. <https://doi.org/10.1002/jsfa.11533>

- Brewer S., Pearson S., Maull R., Godsiff P., Frey J. G., Zisman A. et al. A Trust Framework for Digital Food Systems // *Nature Food*. 2021. Vol. 2, no. 8. P. 543—545. <https://doi.org/10.1038/s43016-021-00346-1>
- Bronson K., Knezevic I. The Digital Divide and How It Matters for Canadian Food System Equity // *Canadian Journal of Communication*. 2019. Vol. 44, no. 2. P. 63—68. <https://doi.org/10.22230/cjc.2019v44n2a3489>
- Carolan M. *The Real Cost of Cheap Food*. New York : Routledge, 2018.
- Chiu Y.-C., Li F.-Y. Effects of the Digital Divide on the Prevention of Food Risk in Taiwan // *Health Promotion International*. 2021. Vol. 37, no. 2. Article 125. <https://doi.org/10.1093/heapro/daab125>
- Gatzweiler F. W., von Braun J. Technological and Institutional Innovations for Marginalized Smallholders in Agricultural Development. Cham : Springer, 2016. https://doi.org/10.1007/978-3-319-25718-1_1
- Hargittai E. The Digital Divide and What to Do about It // *New Economy Handbook* / ed. by D. C. Jones. San Diego : Academic Press, 2003. P. 822—841.
- Kruk S. R. L., Kloppenburg S., Toonen H. M., Bush S. R. Digitalizing Environmental Governance for Smallholder Participation in Food Systems // *Earth System Governance*. 2021. Vol. 10. P. 1—9. <https://doi.org/10.1016/j.esg.2021.100125>
- McBratney A., Whelan B., Ancev T., Bouma J. Future Directions of Precision Agriculture // *Precision Agriculture*. 2005. Vol. 6, no. 1. P. 7—23. <https://doi.org/10.1007/s11119-005-0681-8>
- Mutsvairo B., Ragnedda M. Comprehending the Digital Disparities in Africa // *Mapping the Digital Divide in Africa: A Mediated Analysis* / ed. by B. Mutsvairo, M. Ragnedda. Amsterdam : Amsterdam University Press, 2019. P. 13—26. <https://doi.org/10.5117/9789462986855>
- Park S. *Digital Capital*. London : Palgrave Macmillan, 2017.
- Prabha D., Arunachalam R. Mobile Phone Technology: An Impact of Farming Community // *Journal of Pharmacognosy and Phytochemistry*. 2019. Vol. 8. P. 719—721.
- Ragnedda M. Conceptualizing Digital Capital // *Telematics and Informatics*. 2018. Vol. 35, no. 8. P. 2366—2375. <https://doi.org/10.1016/j.tele.2018.10.006>
- Ragnedda M., Muschert G. W. *The Digital Divide: The Internet and Social Inequality in International Perspective*. New York : Routledge, 2013.
- Ragnedda M., Ruii M. L. The Digital Capital: A Boudieusian Perspective on the Digital Divide. Bingley : Emerald, 2020. <https://doi.org/10.1177/1461444819869604>
- Reisdorf B. C., Dutton W. H., Triwibowo W., Nelson M. E. The Unexplored History of Operationalising Digital Divides: A Pilot Study // *Internet Histories*. 2017. Vol. 1, no. 1—2. P. 106—118. <https://doi.org/10.1080/24701475.2017.1311165>
- Rotz S., Gravely E., Mosby I., Duncan E., Finnis E., Horgan M. et al. Automated Pastures and the Digital Divide: How Agricultural Technologies Are Shaping Labour and Rural Communities // *Journal of Rural Studies*. 2019. Vol. 68. P. 112—122. <https://doi.org/10.1016/j.jrurstud.2019.01.023>
- Tsatsou P. Digital Divides Revisited: What Is New about Divides and Their Research? // *Media, Culture & Society*. 2011. No. 33. P. 317—331. <https://doi.org/10.1177/0163443710393865>
- Upadhyaya L., Burman R. R., Sangeetha V., Lenin V., Sharma J. P., Dash S. Digital Inclusion: Strategies to Bridge Digital Divide in Farming Community // *Journal of Agricultural Science and Technology*. 2019. Vol. 21, no. 5. P. 1079—1089.
- Upadhyaya L., Burman R. R., Sangeetha V., Lenin V., Sharma J. P., Dash S. Factors Affecting Digital Divide in ICT-led Agricultural Information Delivery: A Comparative Analysis // *Agricultural Sciences*. 2018. Vol. 10, no. 1. P. 47—50. <https://doi.org/10.5958/2394-4471.2018.00007.2>
- Van Deursen A. J. A. M., Helsper E. J. The Third Level Digital Divide: Who Benefits Most from Being Online? // *Communication and Information Technologies Annual: Digital Distinctions and Inequalities (Studies in Media and Communications)*. Vol. 10. Bingley : Emerald, 2015. P. 29—52. <https://doi.org/10.1108/S2050-206020150000010002>
- Van Dijk J. *The Deepening Divide: Inequality in the Information Society*. Thousand Oaks : Sage, 2005.
- Van Dijk J. *The Digital Divide*. Cambridge : Polity, 2020.
- Van Dijk J. *The Network Society*. London : SAGE, 2012.
- Weersink A., Fraser E., Pannell D., Duncan E., Rotz S. Opportunities and Challenges for Big Data in Agricultural and Environmental Analysis // *Annual Review of Resource Economics*. 2018. Vol. 10, no. 1. P. 19—37. <https://doi.org/10.1146/annurev-resource-100516-053654>

Сведения об авторах: Ревенко Лилия Сергеевна — доктор экономических наук, профессор кафедры международных экономических отношений и внешнеэкономических связей им. Н.Н. Ливенцева, МГИМО МИД России; ORCID: 0000-0002-1519-1183; e-mail: l.revenko@inno.mgimo.ru

Ревенко Николай Сергеевич — кандидат политических наук, ведущий научный сотрудник Института исследований международных экономических отношений Финансового университета при Правительстве Российской Федерации; ORCID: 0000-0002-0359-5201; e-mail: nsrevenko@fa.ru



DOI: 10.22363/2313-0660-2022-22-2-385-396

Research article / Научная статья

Technology Policy and Sustainable Development in Nigeria

Ejiroghene A. Oghuvbu ✉, Daniel E. Gberevbie , Samuel O. Oni 

Covenant University, Ota, Nigeria

✉augustine.oghuvbupgs@stu.cu.edu.ng

Abstract. In the 21st century, the government and people of Nigeria are placing special emphasis on the technological component of development. In today's world, technology has a critical impact on people and all areas of societal development, from communications and transport to construction and health care. In this study, the term “technology” is used in a broad context, referring to the knowledge, competencies and skills strongly required for technological development. Methodologically, the research is based on the secondary sources — monographs, academic articles and Internet resources. The main idea of the research is to comprehensively analyze the Nigeria's technology and sustainable development policies. The performance of these efforts has been rather poor, preventing Nigeria from reaching a technological level comparable with that of developed economies. Rich in mineral resources Nigeria must initiate the development and adoption of modern technology to accelerate its economic growth. A review of Nigeria's technology policy in the context of a long-term development is required. With a more thorough approach to the development of production functions and operations, such as quality control, maintenance, planning, etc., the level of national development would be much higher than at present. In the case of Nigeria, qualitative improvements in industrial production are directly linked to such factors as knowledge, expertise and experience. Overall, the authors conclude that vocational training for the sub-Saharan Africa sub-region is the key to bringing the respective countries to a new level of technological development. Meanwhile, in seeking technology, Nigeria must strive to strike a balance between industrial development and the environment in order to achieve sustainability.

Key words: technology, technology policy, sustainable development, Nigeria

For citation: Oghuvbu, E. A., Gberevbie, D. E., & Oni, S. O. (2022). Technology policy and sustainable development in Nigeria. *Vestnik RUDN. International Relations*, 22(2), 385—396. <https://doi.org/10.22363/2313-0660-2022-22-2-385-396>

Технологическая политика и устойчивое развитие в Нигерии

Э.А. Огуббу ✉, Д.Э. Гберевбие , С.О. Они 

Университет Ковенант, Ота, Нигерия

✉augustine.oghuvbupgs@stu.cu.edu.ng

Аннотация. В XXI в. правительство и население Нигерии делают особую ставку на технологический компонент развития. В современном мире технологии оказывают наибольшее воздействие на людей и все сферы общественного развития — от коммуникаций и транспорта до строительства и здравоохранения. В рамках данного исследования термин «технологии» используется в широком контексте, в том числе применительно к сфере знаний, компетенций и навыков, необходимых для технологического развития. Методологически исследование основывается на анализе вторичных источников — монографий, научных статей, интернет-ресурсов. Главный акцент сделан на изучении политики Нигерии в сфере технологическо-

© Oghuvbu E.A., Gberevbie D.E., Oni S.O., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

го и устойчивого развития. Страна, располагающая богатыми минеральными ресурсами, для ускорения темпов экономического роста должна инициировать разработку и внедрение современных технологий. Однако результативность прилагаемых усилий довольно низкая, что не позволяет выйти на сопоставимый с развитыми экономиками технологический уровень. В этой связи требуется пересмотр технологической политики в контексте долгосрочного развития Нигерии. При более основательном подходе к развитию производственных функций и операций, таких как контроль качества, техническое обслуживание, планирование и др., уровень национального развития был бы гораздо выше нынешнего. В случае с Нигерией качественное улучшение промышленного производства напрямую связано с такими факторами, как знания и опыт. В целом авторы приходят к выводу, что профессиональное техническое обучение населения субрегиона Африки южнее Сахары является залогом выхода стран на новый технологический уровень развития. При этом в борьбе за технологии Нигерия должна стремиться к обеспечению баланса между развитием промышленности и состоянием окружающей среды для достижения устойчивости.

Ключевые слова: технологии, технологическая политика, устойчивое развитие, Нигерия

Для цитирования: *Oghuvbu E. A., Gberevbie D. E., Oni S. O. Technology Policy and Sustainable Development in Nigeria // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 385—396. <https://doi.org/10.22363/2313-0660-2022-22-2-385-396>*

Introduction

To fully understand technology, one requires knowledge of the technology itself. Therefore, the term “technology” encompasses not only university technical disciplines and special equipment, but also the knowledge and the expertise needed to perform most functions in a modern enterprise. This knowledge includes technical skills, ideas, and equipment that enterprises apply to manufacture and market goods or deliver services.

In the 21st century, technology arguably has the most profound impact on individuals and society. In the case of Nigeria, the technological factor has become truly important in terms of economic development. The daily lives of people in Nigeria are largely determined by the technology used for housing, transportation, office and manufacturing, health care, entertainment and communications. Nigeria’s policy makers expected industrial development to transform low-technology, low-productivity and slow-growth economies into dynamic and modern ones. However, this has not yet happened in the sub-region (Eckardt, 2014).

The logic of exporting technology from those who have it to others who do not is appealing. Most Nigerian leaders believed that the rise of manufacturing was driven by the belief that modern technology and new talent would change the structure of comparative advantages. Past industrial programs tended to focus on increasing production capacity rather

than establishing institutional systems and boosting local capacity to make these facilities more efficient. It is important to bear in mind that most of Nigeria’s post-independence enterprises were capital-intensive and built as turnkey projects by foreign companies, with little transfer of technological capacity to local managers and technicians (Mukoro, 2020).

One of the major problems confronting research in Nigeria is the lack of reliable data, statistics, and documentation on almost every aspect of life in the country. Public institutions, whose work is significantly affected by this fact, nevertheless make so little effort to rectify the situation. In the past, industrialization policies and strategies in Nigeria have discriminated against small and medium-size industries, leaving them without access to credit and foreign exchange.

Nigeria is gradually beginning to recognize the vital role of science and technology as the primary vehicle for promoting development. But this recognition has not been matched with investment in the necessary resources, both human and material. Funding of science and technology in the country has never been any significant priority and has often occurred as a result of external intervention rather than a conviction of its appropriateness and necessity. In addition, science and technology remain largely in the public domain, where they are perceived mainly in terms of building research institutions or developing a technical manpower.

In the latter case, the emphasis is usually placed on formal technical training rather than on building skills, practical experience, and innovation. Unfortunately, policy-makers in Nigeria continue to have a vague understanding of the role of science and technology and have thus failed to optimize their use for national development planning. As a result, many African scholars emphasize that there is a distinct lack of political consciousness and commitment to the development of science and technology (Adubifa, 1990; Lall & Wangwe, 1998; Mukoro, 2019; Udo & Edoho, 2000).

Improving technology is one of the critical factors needed for the industrialization of Nigeria, a goal that seems to be shared by almost everyone. However, the sub-industrial region's activity structure is still underdeveloped. In contrast to Asia and Latin America, which have expanded and deepened their range of more sophisticated operations, the country is dominated by processing of local natural resources and simple consumer goods sectors. The country's industry has therefore failed to achieve structural transformation, export dynamism or technical efficiency, delivering only a fraction of the promised growth and externalities. Some scholars are concerned that Nigeria is on a collision course with resource scarcity and environmental degradation. This concern has led to the concept of sustainability, to ensure that future generations in Nigeria are not deprived of a critical part of their heritage. However, sustainability is a complex and ambiguous concept that is difficult to translate into actual practice (Lawal & Oluwatoyin, 2011; Lipumba, 1994).

A qualitative research methodology has been adopted for this study, as it is aiming to analyze technology policy and sustainable development in Nigeria, which will help to look at the state of technology in Nigeria in the 21st century. The author examines the problem of technology development in Nigeria. Exporting appropriate technology will provide Nigeria with the necessary skills to make rational investment decisions and lead to sustainable growth and development thereafter. In the process of seeking technology the Nigerian government should

endeavor to balance industrial promotion and environmental conditions in order to achieve sustainability. Suggestions are offered on how Nigeria can improve its technology.

Sustainability and Technology Development

Technology in general refers to the various components of productive knowledge that assist in converting raw materials into finished products, developing new and improved products, and developing better and more efficient methods of service delivery. The evolution of technology in Nigeria has elements of history and natural endowment, culture and national discipline. It also has factors of environment and collective national aspiration, elements of knowledge and resourcefulness, and factors of politics and ideology (Soares, Kovaleski, Gaia & Chiroli, 2020).

Thus, technology can be seen as the interaction of science and society. In doing so, it is important to define the understanding of sustainability or sustainable development. It is "a transformation process in which resource exploitation, investment direction, technical development orientation, and institutional change are all in sync and increase both current and future potential to meet human wants and ambitions" (Soares, Kovaleski, Gaia & Chiroli, 2020).

In developing countries, finding alternatives to many of the development practices that are now draining their resources is a key component of sustainable development. Knapper (2016) pointed out that sustainable development in developed countries simply means reducing consumption. This would require developing plans for more efficient use of the current resources, as well as exploiting more fully the solar, wind and thermal energy sources. Both Nigeria and Western industrial countries could cooperate to develop policies that meet basic human needs around the world.

Sustainable development may seem to some, especially in Nigeria, to be an abstract concept of interest primarily to industrialized countries that can afford to worry about such things. Proponents insist that the first order of business

is to develop, then to clean up later. However, the problems underlying sustainable development apply to all countries without exception. Contaminated air and water can significantly slow down development, for example by causing health problems or reducing agricultural production. In addition, global warming is likely to hurt Nigeria at least as much as others because highly stressed and barely adequate agricultural systems will have great difficulty adapting to climate changes (Oladipo & Grobler, 2020). It is therefore in the interest of the Nigerian government to position its development in line with the principle of sustainability. “The missing component model is predicated on the idea that development can be affected by identifying the critically weak or missing element in developing a country’s assets and by subsequently providing this component. Such missing elements typically are identified as domestic saving, foreign exchange, education and technology. The capacity of technology to transform nature in Nigeria for the purpose of development is such that the question of who controls technology is central to who controls development” (Udo & Edoho, 2000, p. 120).

The difficulty with a development plan that emphasizes the acquisition of foreign exchange is that it leads to foreign currency dominance and overcapitalization in sub-Saharan Africa at the cost of a more balanced use of domestic resources. One negative consequence can be the overuse of labor as a substitute for capital. Most of the arguments in favor of the concept of appropriate technology are based on this second criterion. The importance of technology efficiency in the development process cannot be overstated. Ultimately, this will prove to be a way for developing countries, such as those in sub-Saharan Africa, to move out of poverty and achieve the goals outlined in the basic human needs approach.¹

As some scholars have pointed out, capacity building is essential for the successful transfer of

¹ Yusuf O., Shogbanmu S. Reigniting Growth and Sustainable Development in Nigeria // Verraki: Business Solutions for Africa. May 2021. URL: https://verraki.africa/wp-content/uploads/2021/05/Reigniting-growth-and-sustainable-development-report_May-2021.pdf (accessed: 23.02.2022). See also: (Yekini, 2014).

new technology to poor countries; simply improving equipment and operating instructions, patents, designs, or blueprints does not guarantee that the technology will be successfully used (Lall, Navaretti, Teitel & Wignaraja, 1994). For Ofori three functional categories of technological capacities are the most important for developing countries to successfully transfer technology (Ofori, 1994). These functional categories include investment capability (skills and information needed to identify and determine feasible investment); production capability (skills, knowledge, and experience imperative for running an operation and improving the plant); linkage capabilities (skills required to create, maintain, and build technology connections with other businesses and institutions).

The use of any technology is not an end in itself. The criteria for making an effective technical decision in Nigeria must be found in the country’s most important development goals and procedures. Mukoro (2020) argues that the description of situations in which technology is applied determines both private and public aspects. The technology used in a small family-owned business is referred to as private technology. It has to do with the manufacture of consumer goods, and it is mostly an individual entrepreneur’s decision. Examples of “public technology” include large industrial firms producing consumer goods or capital equipment, as well as national institutions providing basic services such as rail transport, flood control and irrigation systems, electricity grids, higher education, banking and credit systems. As a result, in Nigeria, technological advances imply new methods that surpass existing national standards, but do not necessarily have to be on top of the world. This is due to the fact that Nigeria is still in the early stages of industrial and agricultural development (Mukoro, 2020).

Sub-Saharan Africa has embraced technology transfer strategy as a principal means of incorporating technical change into their productive structure (Marais, Grobbelaar & De Kock, 2021; Yusuf and Shogbanmu²).

² Ibid.

Technological change, however, is a multi-dimensional phenomenon: it involves changes in the socio-cultural, cognitive, and managerial attributes of society. Transforming changes in the socio-cultural, cognitive and governance attributes of sub-Saharan African societies into a concept of policy sustainability raises important questions about how global social capital or assets should be shared between present and future generations. This capital consists of four components: man-made capital such as roads and factories, scientific and technical knowledge, natural capital such as fossil fuels and mineral deposits, and environmental assets such as clean air and water and a diverse biological base (Marais, Grobbelaar & De Kock, 2021). There is typically little concern over the first two. It is assumed in line with historical experience at least over the past three or four centuries; that each generation will be able to hand down to future generations an improved stock of both technical knowledge and manmade capital. This concern was also addressed by the World Bank and International Monetary Fund (IMF) structural adjustment policies prescription to developing nations in the 1980s and 1990s (Woyo, Rukanda & Nyamapanda, 2020).

As Lipumba (1994) points out, environmental protection was not the original objective of the structural adjustment programs that were prescribed by the World Bank and IMF in the 1980s and adopted by African countries. The aftermath of the programs was that the impact of adjustment on the environment was previously ignored. The promotion of certain exports such as tropical wood and flue-cured tobacco, which was undertaken in some areas as part of the adjustment effort, could result in deforestation. On the balance, there is no good evidence that adjustment policies have had either a positive or negative impact on the environment. Rapid population growth rate and overgrazing are more formidable threats to the environment than adjustment. Overall, the policy challenge for sub-Saharan Africa is to maintain the delicate balance between population growth and agricultural and technological development on the one hand, and the protection of the environment on the other (Niebel, 2018).

The Evolution and the Quest for Technology Transfer

Looking back at the performance of the early colonial officers in terms of their responsibility for national planning and the circumstances in which they functioned is the best way to describe the evolution of technology transfer in Nigeria. The relationship between the colonial heritage and the indigenous civil service after independence, as well as subsequent evolution and change based on the colonial foundation, may then be traced. Before 1960, the colonial civil service in charge of Nigeria was never meant to build or manage industries or the production system. It was simply meant to preserve law and order in the colonial government's interest and promote trade and acquisition of raw materials. During the pre-independence period in Nigeria, there was no clear policy for science and technology. The only policy that was in place was an industrialization plan. This plan was only implicit in nature because the concern of the European colonial authorities was mostly commercial (Soares, Kovaleski, Gaia & Chiroli, 2020). The colonial administration's goal was to promote the development and transfer of agricultural commodities as raw materials for Europe (Knapper, 2016).

The colonial civil service was essential in the entry of foreign firms into Nigeria, rather than directly establishing enterprises. First, multinational firms mostly engaged in commerce and transportation, acquiring and shipping raw materials from the sub-region to developed-country industries. Second, international firms delivered finished goods to the Sub-Saharan African market, particularly textiles and processed foods. Third, international firms later introduced the import-substitution approach, which became the first industrialization process to be implemented domestically in Nigeria (Marais, Grobbelaar & De Kock, 2021; Wangwe, 1995). It could therefore be argued from the outset that the colonial administration was not concerned with the setting-up of industrialization or the provision of infrastructure. The colonial administration also did not create any formal

mechanism for participation in the production system as a function of government.

With independence, Nigeria started to recognize the importance of industrialization as a major vehicle for national development. Unlike other developing countries which had successfully utilized appropriate strategies for their own purpose, the Nigerian government's strategy for industrialization was initially that of total reliance on foreign private investment supported by generous tax rebates and pioneer incentives. Import substitution was the primary objective. The issues above, therefore, point to a certain pattern of technological development that was inappropriate and resulted from policy failures in development planning. By failing to establish centralized coordination of technological activities, the nation achieved a high-cost assortment of desirable and undesirable technological inputs (Gray, 2017).

At present, Nigeria remains a technologically inferior, poor, and dependent economy (Biggs, Shah & Srivastava, 1995; Ihonbere, 1994; Mukoro, 2019). In the context of Africa, however, the structures of the Nigerian economy appear relatively developed, but when viewed on a worldwide basis, they are less so. The fact remains that foreign interests dominate Nigeria's economy, and the society is characterized by a lack of discipline, and corruption, for the vast majority, political instability, ethnic, religious, and regional cleavages, and a general lack of fundamental human requirements exist.

The World Bank has reported a decline in technology development activities in the years following the introduction of the structural adjustment programs. This was reflected in the drop in the fourth quarter of 1999, the aggregate index of industrial production was expected to be 22.8% (1985 taken as 100%). In 1994 and 1995, reductions of 5.0 and 5.1% were observed, respectively. Manufacturing and mining output declined by 8.3 and 9.8% in 1996 and the first quarter of 1997, respectively, contributing to the decline in industrial production. The index decreased by 15.7% in the third quarter of 1998, owing partly to the persisting political instability

in most Sub-Saharan African countries and the difficulty in obtaining foreign cash for the import of raw materials and machinery spare parts. Furthermore, industrial production declined by 1.8% in the first quarter of 2019, 2.5% in the third quarter of 2020, and 2.6% in the third quarter of 2021.³

Generating human resources for effective technology transfer could be done through the development of formal education (Lall, 1999). Industrial training is just as crucial, if not more so. While comparable data isn't accessible, anecdotal evidence shows that Sub-Saharan African countries (particularly Nigeria) (Table 1) lag behind in vocational and technical training. Most industrial companies spend little or no money on employee training, merely giving the rudimentary skills required to run specific technologies. Furthermore, with new technologies and organizational forms, the nature and extent of demand for industrial skills is rapidly changing in the direction of multi-skilling teamwork, reliability and flexibility, and continuous education; the gap between Nigeria and other industrialized nations is widening rather than closing (Yekini, 2014).

Table 1 shows enrollment rates in vocational and technical subjects in universities in some Sub-Saharan African countries in comparison with nations in Asia and Latin America. Vocational and technical training is how high-level human capital for technological transfer and industrial development can be achieved. The table shows that Latin American and Asian countries fare better in the technical and vocational training that they provide for their citizens. The table provides data for South Africa as well as the four relatively advanced less developed African economies, Ghana, Kenya, Zimbabwe, and Nigeria. The other sub-Saharan

³ See: Selassie A. A., Hakobyan S. Six Charts Show the Challenges Faced by Sub-Saharan Africa // IMF. April 15, 2021. URL: <https://www.imf.org/en/News/Articles/2021/04/12/na041521-six-charts-show-the-challenges-faced-by-sub-saharan-africa> (accessed: 23.02.2022); World Development Report 2000/2001: Attacking Poverty // The World Bank. Washington, DC : The World Bank, 2001. P. 296. URL: <https://openknowledge.worldbank.org/handle/10986/11856> (accessed: 23.02.2022).

African countries are very much further behind. South Africa is clearly in front of other sub-Saharan African nations, and it has approached the levels reached in some relatively advanced Asian or Latin American nations.

Table 1

Educational Enrollment at all Levels in Vocational and Technical Subjects at Universities

Country	Vocational training		Enrollment in Technical Field	
	Number	% of population	Number	% of population
Africa				
Ghana	22,578	0.15	712	0.00
Kenya	7,8401	0.04	1,046	0.00
S. Africa	47,801	0.15	19,958	0.06
Zimbabwe	0	0.0	4,718	0.04
Nigeria	20,450	0.12	74,000	3.00
Asia				
Korea	1,483,198	3.33	437,537	0.98
Taiwan	513,700	2.46	179,094	0.86
Singapore	9,391	0.32	13,029	0.47
Malaysia	90.079	0.48	12,693	0.07
Philippines	NA	0	201,701	0.29
Thailand	545,791	0.92	51,949	0.09
Latin America				
Chile	277.226	1.98	85,483	0.61
Mexico	835.079	1.03	221,867	0.27
Argentina	1,084,531	3.22	96,205	0.29
Brazil	1,480,997	0.99	149,660	0.10

Source: (Lall & Wangwe, 1998; Oviawe, 2017).

All the expenditures on research and development (R&D) fell by 0.9% in 1995 and 26.6% in 1996 from the 1985 level. As in previous years, the expenditure on R&D continued to account for a dismal fraction (1.7%) of total investment expenditure in sub-Saharan Africa.⁴ At the end of 1998, the situation in the public and private sectors deteriorated further due to a decline in production and a low overall capacity utilization rate. Poor implementation of structural adjustment programs, insufficient funding, especially for working capital, currency restrictions on the purchase of necessary raw materials and spare parts, high operating costs, frequent equipment breakdowns, and a wave of political instability were blamed for the poor performance.

⁴ Human Development Report 1999 // UNCTAD. New York: Oxford University Press, 1999. URL: https://hdr.undp.org/sites/default/files/reports/260/hdr_1999_en_nostats.pdf (accessed: 23.02.2022).

Finally, technology is still widespread in Nigeria and many sectors of the economy rely on it and are affected and affected by it. Technology also serves as a link between production and employment, as well as between the economic system and the environment. As a result, the development strategy required effective public-private control over technology. Nigeria must be able to choose appropriate items and technology and assure its supply in order to drive the growth process. Suppliers can be discovered through an indigenous design and development efforts or by acquiring goods from overseas and adapting and changing them to match local requirements (Mukoro, 2020).

Only a careful rethinking of Nigeria's goals (the demand side) and means (the supply side) will reconcile technological, social, economic and environmental objectives. Through the use of proper production methods, technology matters to both parties. This requires that Nigeria not only considers technology in terms of capital and labor, but also examines it as a multifaceted entity involving both the public and private sectors (Oladipo & Grobler, 2020).

Nigeria is abundant in natural resources which should after over six decades of independence transcend into technological development. But the country is still far from been able to compete with other nations despite its huge natural endowment. Nigeria still has significant access gaps, with over 25 million people without access to any sort of telephone service. Despite the fact that the sector has connected 289 million lines, 199 million of which are operational. This is a huge improvement over the mere 400,000 lines supplied by the now-defunct Nigerian Telecommunication Limited (NITEL) between 1985 and 2001, just before the telecommunications revolution that gave birth to MTN, *Globacom*, *Airtel*, and *9mobile*. While many sectors of the economy have been hit hard by the COVID-19 pandemic which ravaged the world, according to the National Bureau of Statistics (NBS), Nigeria's telecommunications and information services sector remains optimistic as a driver of economic growth, contributing NGN 2.3 trillion or 14.3% of GDP in the second quarter of 2020 (Huang, 2021). The contribution of telecoms to GDP was 8% in

2015, but it has increased dramatically quarter over quarter and year over year to reach the present milestone of 14.3% in the second quarter of 2020. Today, many Nigerians can say that the online world has presented them with opportunities to do business. According to the Nigerian Communications Commission (NCC), 147 million Nigerians use the Internet. It's also worth noting that the sector's investment has surpassed USD 80 billion (Huang, 2021).

Nigeria remains mostly a consumer country. Nigeria's annual importation of IT solutions is projected to be in excess of USD 2 billion. The country's hardware industry is 80 per cent foreign-owned. The country's technological prowess remains pitiful. Nigeria, for example, has regularly ranked worst in the Global Innovation Index (GII) over the last seven years, and had not fared much better before that. Nigeria was placed 114th out of 129 economies in the 2019 GI. It was ranked 118th a year ago.⁵

Exporting Technology for Sustainable Development

Marais, Grobelaar, and De Kock (2021) identified four components of the technology transfer strategy for Sub-Saharan Africa (including Nigeria). These policies include importing technology, upgrading the capacities of small and medium-sized businesses, strengthening technology infrastructure, and increasing the level of technological effort by large corporations (Table 2). Technology exported into Nigeria has imported capital goods that have generally played a role. To strengthen and deepen the industrial structure, it is critical to stimulate technology imports, particularly through foreign direct investment, as well as to encourage local enterprises to upgrade their skills and capacities by absorbing the firm's beneficial spillovers. Individuals in Nigeria in a matter should direct industrial policy that it will provide strong technical support to small and medium-sized enterprises. More technology transfer

would be facilitated by offering agency services for technology transfer and development, supporting training and information search initiatives, and giving assistance for management and consultancy services (Mukoro, 2020). Furthermore, in order to meet the technological requirements of a more open and competitive marketplace, policies to modernize the technological infrastructure need to be developed. The quality and reach of technological infrastructure services could be critical in boosting quality, launching successful inventions, and breaking into new export markets in the future of the twenty-first century.

The Nigerian government needs to introduce policies that would help promote R&D (Dibie, 1997). As the industry progresses into more complicated technologies, R&D capability becomes increasingly important in order to assimilate foreign technology. As a result, industrial policy should be intended to encourage long-term investments in R&D, as well as the development of the necessary skill set. Lall, Navaretti, Teitel, and Wignaraja (1994) and Udo and Edoho (2000) contend that investment, production, and linkage capabilities are very important for the sub-Saharan African (including Nigerian) institutions to develop sustainable growth (see Table 2). Nigeria's investment capabilities are the skills and information it needs to find and purchase appropriate technologies, build and engineer factories, oversee construction commissioning, and begin the manufacturing process. Udo and Edoho (2000) pointed out that in most cases this task is contracted out to international consultants. As a result, the opportunity to develop investment capabilities is lost. The Nigerian government also needs production capabilities in the form of knowledge and experience. This is very imperative for them to run an operation and improve the production plants. Nigeria would go a long way if it could develop basic production capabilities such as quality control, maintenance, scheduling, and so on.

Linkage capabilities have to do with the elaborate networks of cooperative relationships with suppliers, buyers, and governments. It also requires Nigeria to have managers with the requisite level of skills to make rational

⁵ Yusuf O., Shogbanmu S. Reigniting Growth and Sustainable Development in Nigeria // Verraki: Business Solutions for Africa. May 2021. URL: https://verraki.africa/wp-content/uploads/2021/05/Reigniting-growth-and-sustainable-development-report_May-2021.pdf (accessed: 23.02.2022). See also: (Huang, 2021).

investment decisions and improve their core managerial functions. Building administrative and management competence is a critical component of a successful technology transfer. Poor management capacity as well as a weak institutional and administrative structure continue to stymie the creation and execution of science and technology policy in Nigeria. The government servant is frequently overworked and underpaid, making it difficult to be efficient and respond quickly to changing conditions. As a vital component of capacity-building initiatives, a knowledgeable, better-trained, and motivated civil service with a performance-based remuneration structure, as well as increasing decentralization and delegation of tasks, should be built as efficiently and cost-effectively as possible. Capacity building should therefore extend to the private sector through the creation of relevant institutions, including measures to boost the role of non-governmental organizations and to enable women to fully engage in the process of technological transformation and sustainable growth (Lawal & Oluwatoyin, 2011).

Thus, upgrading management know-how among men and women in both public and private sectors will provide the needed impetus for economic growth and sustainable progress in Nigeria. Appropriate technology transfer and sustainability in Nigeria means that renewable resources must replace depleting ones. Sustainability of technology also implies improving the efficiency with which energy is used, reducing the environmental degradation caused by conventional energy production and use, and moving towards greater reliance on sources that do not produce carbon dioxide. Although this is an ambitious program for Nigeria that will involve many changes in policies and institutions; much of the technology is already available or close to commercial readiness (Gray, 2017). Over the past twenty years, great advances have been made worldwide in the development of these technologies. Nations such as Nigeria that lack well-developed energy networks are most likely to find the adoption of renewables to be advantageous. Ofori (1994) pointed out that it was of everyone's interest to ensure that renewables be used whenever practical because that would help

reduce emissions of carbon dioxide, lower costs, builds a market, improve energy reliability, and actual technologies, some important countries may benefit from policy advice to allow renewables to compete on more equal terms. Table 2 shows two approaches to sustainable technology development in Nigeria.

Table 2

Approaches to Sustainable Technology Transfer

Sustainable technology transfer and development	
Education in vocational, technical and managerial skills	Upgrade small and medium size enterprises
Investment capabilities	Import technology
Production capabilities	Improving the technology infrastructure
Linkages capabilities	Policies to promote research and development
Political will and diplomatic expertise	Use renewable resources

Source: (Ofori, 1994).

Before investing or expanding their technological manufacturing, entrepreneurs require a stable business climate. The first step toward reducing entrepreneur uncertainty and ensuring the stability of regulatory and institutional reforms is to include representative associations in the policy-making process. This conversation necessitates a shift of mindset on everyone's part. Policymakers must recognize the private sector's vital role and refrain from taking arbitrary acts that stifle its operations. Associations should be encouraged to participate in the regulatory and institutional reform process through structural adjustment measures that facilitate broad-based dialogue. Entrepreneurs, for their part, should learn to compete and produce efficiently on a fair playing field, where long-term success is determined by the capacity to compete and produce efficiently rather by privilege or evasion. Other government measures should include efforts to encourage new entrepreneurs, as well as efforts to retain existing economic activity and expand creative businesses. Economic growth should be channeled into particular areas as part of policies to deal with the land use component of development (Dibie, 1997; Woyo, Rukanda & Nyamapanda, 2020). The plan would also include features relevant to site acquisition and development if the state or community chooses to take a direct entrepreneurial role, for example.

Sub-Saharan African countries should consider financing and encouraging entrepreneurs in high-tech fields.

In Sub-Saharan Africa excessive bureaucratic meddling creates lawlessness. It motivates businesses to find loopholes in the regulations, causing those who follow them to lose their competitive advantage. Getting rid of onerous restrictions will help to reduce the hidden costs that many entrepreneurs face when it comes to obtaining permits and registering their businesses. Bribes are only one type of expense; long delays and convoluted procedures incur additional costs in terms of lost productivity and competitiveness. If small-scale companies are to thrive, licensing and other requirements must be thoroughly evaluated and only preserved if there is strong justification (Knapper, 2016).

Protecting young businesses from international competition with tariffs may not be the best idea; instead, the government should limit foreign investment in some sectors. Nigeria's industrial efficiency will be improved by importing from technologically sophisticated economies. The government, on the other hand, should encourage local engineers and technicians to import a foreign machine, disassemble it, study how it was built, and alter it to match local conditions. According to the product-cycle method, technical borrowing can progress from an imported product to a duplicate, which is usually of lower quality, to a gradual development, with finer grades and specialties, which come with experience and increased human and physical capital endowment. Future studies could look into how increased entrepreneurial behavior can help Nigeria's economy grow. Nigeria's competitive advantage will be shifted with this method (Mukoro, 2019). Technology export is primarily an information process among people. It provides information for improving designs or the production of goods and services. It need not involve the sale of equipment, but sales can incorporate technology transfer in the form of training and additional information to give the recipient new capabilities. Education is an important form as attested to by the thousands of Chinese students studying technical subjects in American universities (Lawal & Oluwatoyin, 2011).

Companies clone most technology export from the United States because it is often a prerequisite for sales. In addition to training, it can involve licensing for production, joint ventures, co-production, and other forms. The United States government transfers technology through access to information, assistance with regulation and other activities such as development assistance or educational programs. These efforts are seen as being in the United States' national interests because they are effective ways to promote development and cultivate political and economic ties. Significant progress toward sustainability will be made only when appropriate technologies discussed in the previous section are widely available, well understood, and advantageous compared to alternatives. To be affordable, much of the equipment must be produced in developing countries, and much of the technology is well within their capabilities. China has been a world leader in the production of small hydropower equipment. Other technologies will require technology transfer for developing countries to assimilate designs and achieve adequate quality control. In addition to the physical equipment, transfer of technical and political expertise may be necessary to create adequate environmental and energy institutions, so that appropriate selections of technology can be made. A wide variety of companies are involved with technologies appropriate for sustainability. Large, international companies are well acquainted with technology transfer. For example, the nuclear industry originated in the United States, and the technology was deliberately transferred abroad (Eckardt, 2014; Niebel, 2018; Yekini, 2014).

Conclusion

This study explores the problem of technology development in Nigeria and looks at ways of exporting technology for sustainable development. It highlights the relevance of technology as a major driver of economic and structural transformation in Nigeria. The authors argue that in seeking technology sub-Saharan governments should endeavor to balance industrial promotion and environmental conditions in order to achieve sustainability. The

pre-independence colonial administration built the economy around extracting raw materials for European industry and private foreign interests, which caused a delay in developing a solid technological base in Nigeria. In their business interactions with Nigeria, foreign investors are neither humane nor philanthropic. They have been egoistic and selfish; preferring to prioritize their own interests over upholding high moral standards and assisting Nigeria in developing a sustainable economy. With a particular reference to the interplay of public and private investment in technology, a crucial problem lies in the persistent drain or the siphoning by foreign investors of resources away from Nigeria. The point here is that imported private technology has contributed little to technological progress in Nigeria. Another perspective is that Nigeria has failed to take advantage of previously imported superior technology to create a technology system that is acceptable to itself.

Two approaches to technology transfer and sustainable development are proposed in this study. On the one hand, Nigeria's acquisition of appropriate technologies requires education in professional, technical and managerial skills, investment, production and networking opportunities, the use of renewable energy, and political will and diplomatic experience. On the other hand, technology imports, upgrading small and medium-size enterprises, improved technological infrastructure, policies promoting research and development and the use of

renewable resources are all important factors that will enable sub-Saharan African countries to achieve technological transfer and sustainable development.

It is very important that the Nigerian government seeks to balance technological development, industrial development and environmental conditions to achieve sustainability. Enterprises begin with people; therefore, the governments in the sub-region should provide technical and vocational training for their citizens. Future development policies must acknowledge that while governments can help, people are the ones who make things happen. The Nigerian government also needs a healthy business climate that allows it to prepare for the future, rewards efficiency and encourages entrepreneurs to invest in themselves and their businesses. They require financial and information systems that provide access to resources, as well as infrastructure that enables them to connect to the rest of the economy and organizations that promote human resource development. Donors can make a significant contribution to these efforts by working with governments and local organizations to enhance business and encourage entrepreneurial capacity. In addition to physical equipment, technology transfer and policy expertise may be needed to create adequate environmental policies and institutions, so that appropriate technology choices can be made in the future.

Received / Поступила в редакцию: 22.02.2022

Revised / Доработана после рецензирования: 13.03.2022

Accepted / Принята к публикации: 18.04.2022

References / Библиографический список

- Adebifa, A. (1990). *Technology policy in Nigeria*. Ibadan: NISER Publications.
- Biggs, T., Shah, M., & Srivastava, P. (1995). *Technological capability and learning in Africa enterprises*. Washington, DC: The World Bank.
- Dibie, R. (1997). Business — government relations and technology development in Nigeria. *Journal of Developing Societies*, 13(2), 195—207.
- Eckardt, M. (2014). The impact of ICT on policies, politics and polities: An evolutionary economics approach to information and communication technologies. *Andrassy Working Paper Series*, (32), 1—19. Retrieved from <https://www.andrassyuni.eu/pubfile/de-223-awp32eckardtfinal.pdf>
- Gray, S. L. (2017). The social construction of time in contemporary education: implications for technology, equality and Bernstein's 'conditions for democracy'. *British Journal of Sociology of Education*, 38(1), 60—71. <https://doi.org/10.1080/01425692.2016.1234366>
- Huang, Y. (2021). Technology innovation and sustainability: Challenges and research needs. *Clean Technologies and Environmental Policy*, 23, 1663—1664. <https://doi.org/10.1007/s10098-021-02152-6>

- Ihonvbere, J. O. (1994). *Nigeria: The politics of adjustment and democracy*. New Brunswick: Transaction Publishers.
- Knapper, C. (2016). Does educational development matter? *International Journal for Academic Development*, 21(2), 105—115. <https://doi.org/10.1080/1360144X.2016.1170098>
- Lall, S, Navaretti, G. B., Teitel, S., & Wignaraja, G. (1994). *Technology and enterprise development: Ghana under structural adjustment*. London: Palgrave Macmillan. <https://doi.org/10.1007/978-1-349-13925-5>
- Lall, S. (Ed.). (1999). *The technological response to import liberalization in Sub-Saharan Africa*. London: Palgrave Macmillan.
- Lall, S., & Wangwe, S. (1998). Industrial policy and industrialization in Sub-Saharan Africa. *Journal of African Economics*, 7(1), 70—107. https://doi.org/10.1093/jafeco/7.suppl_1.70
- Lawal, T. & Oluwatoyin, A. (2011). National development in Nigeria: Issues, challenges and prospects. *Journal of Public Administration and Policy Research*, 3(9), 237—241.
- Lipumba, N. H. I. (1994). *Africa beyond adjustment*. Washington, DC: Overseas Development Council Series.
- Marais, R.; Grobbelaar, S. S., & De Kock, I. H. (2021). Healthcare technology transfer in Sub-Saharan Africa: Conceptual framework evaluation. *IEEE-Transactions on Engineering Management*, 1—17. <https://doi.org/10.1109/TEM.2021.3109445>
- Mukoro, A. (2019). *Public administration: Practice and theory in Nigeria*. Ibadan: Ababa Press Ltd.
- Mukoro, A. (2020). *Administration of the public service*. Ibadan: Ababa Press Ltd.
- Niebel, T. (2018). ICT and economic growth: Comparing developing, emerging and developed countries. *World Development*, 104, 197—211. <https://doi.org/10.1016/j.worlddev.2017.11.024>
- Ofori, G. (1994). Construction industry development: Role of technology transfer. *Construction Management and Economics*, 12(5), 379—392. <https://doi.org/10.1080/01446199400000049>
- Oladipo, O. D., & Grobler, W. (2020). Information and communication technology penetration level as an impetus for economic growth and development in Africa. *Economic Research — Ekonomiska Istraživanja*, 33(1), 1394—1418. <https://doi.org/10.1080/1331677X.2020.1745661>
- Oviawe, J. I. (2017). Fostering students' enrolment in technical education programmes through career guidance and occupational awareness. *Education Journal*, 6(4), 125—132. <https://doi.org/10.11648/j.edu.20170604.11>
- Soares, A. M., Kovaleski, J., Gaia, S., & Chiroli, D. M. (2020). Building sustainable development through technology transfer offices: An approach based on levels of maturity. *Sustainability*, 12(5), 1—22. <https://doi.org/10.3390/su12051795>
- Udo, G. J., & Edoho, F. M. (2000). Information technology transfer to African nations: An economic development mandate. *Journal of Technology Transfer*, 25, 329—342. <https://doi.org/10.1023/A:1007886908690>
- Wangwe, S. M. (Ed.). (1995). *Exporting Africa: Technology, trade and industrialization in Sub-Saharan Africa*. London: Routledge.
- Woyo, E., Rukanda, G. D., & Nyamapanda, Z. (2020). ICT policy implementation in higher education in Namibia: A survey of students' perceptions. *Education and Information Technologies*, 25(5), 3705—3722. <https://doi.org/10.1007/s10639-020-10118-2>
- Yekini, N. A. (2014). *Information communication technology: Concepts and application*. Lagos: Hasfem Publishers.

About the authors: *Oghuvbu Ejiroghene A.* — PhD Student, Department of Political Science and International Relations, Covenant University; ORCID: 0000-0003-1422-3806; e-mail: augustine.oghuvbupgs@stu.cu.edu.ng
Gberevbie Daniel E. — PhD, Professor, Department of Political Science and International Relations, College of Leadership Development Studies, Covenant University; ORCID: 0000-0002-3958-2699; e-mail: daniel.gberevbie@covenantuniversity.edu.ng
Oni Samuel O. — PhD, Associate Professor, Department of Political Science and International Relations, College of Leadership Development Studies, Covenant University; ORCID: 0000-0003-3513-0844; e-mail: Samuel.oni@covenantuniversity.edu.ng

Сведения об авторах: *Огубву Эджирогене А.* — аспирант департамента политической науки и международных отношений Университета Ковенант; ORCID: 0000-0003-1422-3806; e-mail: augustine.oghuvbupgs@stu.cu.edu.ng
Гберевбие Даниэл Э. — доктор наук (PhD), профессор департамента политической науки и международных отношений Университета Ковенант; ORCID: 0000-0002-3958-2699; e-mail: daniel.gberevbie@covenantuniversity.edu.ng
Они Самуэл О. — доктор наук (PhD), доцент департамента политической науки и международных отношений Университета Ковенант; ORCID: 0000-0003-3513-0844; e-mail: samuel.oni@covenantuniversity.edu.ng



МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ INTERNATIONAL SECURITY

DOI: 10.22363/2313-0660-2022-22-2-397-410

Research article / Научная статья

Space and Counter-Space Activities of Great Powers in Outer Space

Md Badrul Islam  

Bangabandhu Sheikh Mujibur Rahman Science & Technology University, Gopalganj, Bangladesh

 badrul.islam@bsmrstu.edu.bd

Abstract. The article is dedicated to outer space as a space, including the Moon and other celestial bodies, open for exploration and use by all. Celestial bodies are natural resources of the common heritage of humanity. Their exploration and use for the benefit and discovery of all countries is the result of the ownership of all mankind. However, since the end of the 20th century and especially in the 21st century, outer space has gradually become militarized. This is due to changes in the system of warfare, which is likely to be heavily transformed in the coming future. In this transformational system, all domains of warfare will be interlinked and outer space will play a significant role. One example of such processes is the Gulf War, also called the First Space War, in which the US Army successfully used the outer space systems for its Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) activities. Since then, outer space has become an integral part of US military operations. Consequently, other great powers like Russian Federation and People's Republic of China are also trying to develop the same capability to counter US dominance in outer space. Simultaneously, the US is continuing its counter-space capabilities to maintain the dominance in outer space. The growing dependence on outer space is not only applicable to the military operation but also to commercial and civilian activities. As a result, great powers are more actively engaging in various space and counter-space activities to pursue their national interests; such activity turns outer space into an arena for inter-state rivalry.

Key words: security, outer space, great power competition, Russia, USA, China

For citation: Islam, M. B. (2022). Space and counter-space activities of great powers in outer space. *Vestnik RUDN. International Relations*, 22(2), 397—410. <https://doi.org/10.22363/2313-0660-2022-22-2-397-410>

Космическая и противокосмическая деятельность великих держав в космосе

М.Б. Ислам  

Научно-технический университет имени Бангабандху Шейха Муджибура Рахмана, Гопалгандж, Бангладеш

 badrul.islam@bsmrstu.edu.bd

Аннотация. Рассматривается космос, включая Луну и иные небесные тела, в качестве пространства, открытого для исследования и использования всеми государствами, поскольку небесные тела — это природные ресурсы, являющиеся общим наследием человечества. Их исследование и использование на благо и для

© Islam M.B., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

открытия всех стран является результатом права собственности всего человечества. Проанализированы аспекты милитаризации космического пространства великими державами, в частности США, Россией и Китаем, в конце XX — начале XXI в. Этот процесс связан с изменениями в способах ведения боевых действий, в результате чего формируется новая система проведения военных операций в различных пространствах, взаимосвязанных друг с другом через космическое пространство. Одним из примеров является война в Персидском заливе, также известная как Первая «космическая» война, в которой американская армия успешно использовала свои спутниковые системы для тестирования автоматизированной системы управления войсками (АСУВ). С тех пор космическое пространство стало неотъемлемой частью военных операций США. Россия и Китай также пытаются развивать аналогичные системы и возможности для противодействия господству США в космосе. При этом США продолжают совершенствовать свои контркосмические возможности для сохранения превосходства в космическом пространстве. Растущая зависимость от космоса характерна не только для военных операций, но и коммерческой и гражданской деятельности. Также великие державы в целях реализации своих национальных интересов инициатируют различные космические и контркосмические мероприятия, что превращает космос в арену межгосударственного противостояния.

Ключевые слова: безопасность, космическое пространство, великодержавная конкуренция, Россия, США, КНР

Для цитирования: *Islam M. B. Space and Counter-Space Activities of Great Powers in Outer Space // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 397—410. <https://doi.org/10.22363/2313-0660-2022-22-2-397-410>*

Introduction

Great powers competition across the various domains of warfare is not a new phenomenon. In ancient times state contests took place on land. Then, in the medieval period, water was added as another field of conflict. The early 20th century is marked by aggressive rivalries among the great powers, mainly Great Britain, the United States, Japan, Germany, the USSR, Italy and France, for controlling land, water and air, which culminated in two World Wars. During the Cold War the United States and the USSR discovered a new sphere of dominance — outer space. Throughout the Cold War both parties pursued new ways of utilizing space to extend their nuclear deterrence, strategic stability, early warning, and command and control system. In the post-cold war era, the new goal was fixed — to find out the ways through which space could contribute to military operations in wartime. The Gulf War of 1991 saw an unprecedented rise of the military value of space systems through the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) system. Additionally, the non-military usage of outer space for communication, weather forecast, financial transaction, navigation and a potential source of natural resources rendered it extensive importance to all countries. Consequently, in the 21st century satellites have become an integral part of both

civilian and military utilization. Nearly 50 states and multinational organizations own and operate more than 2000 satellites as of 2021.¹

The fall of the USSR and the tremendous technological progress along with increasing economic capabilities have made the United States more powerful in outer space than any other nation. However, the technological progress of China and the reemergence of Russia as a successor of the USSR have created challenges to US dominance. At the same time the rise of India and Japan in space technology pose a threat to the Chinese rise in outer space. The successful anti-satellite weapons (ASAT) tests by China, US and Russia in 2007, 2008 and 2018 respectively as part of their counter space operations further reinforced such competition. Hence, this article is intended to analyze the great power activities in outer space. The article begins with a historical discussion of space competition. Then it explains the strategic importance of outer space. Despite various competitive actions among different states, this research focuses on the endeavours of the US, Russia and China, the most noticeable ones, in controlling the outer space. Looking forward,

¹ Salas E. B. Number of Satellites in Orbit by Country as of January 1, 2021 // Statista. July 21, 2021. URL: <https://www.statista.com/statistics/264472/number-of-satellites-in-orbit-by-operating-country/> (accessed: 31.01.2022).

this paper attempts to forecast the future implications of space competitive landscape.

History of the Cold War Outer Space Competition

The USSR launched the world's first satellite, Sputnik, on October 4th, 1957 and then sent the first human, Yuri Gagarin, to space in 1961. These achievements put the Soviet Union ahead in the space race and at the time, were considered humiliating to the United States. Hence, the National Aeronautics and Space Administration (NASA), the center of the US space research agency, was built in 1958 in reaction to Soviet space progress. In 1962, US President John F. Kennedy expressed the country's ambitions in space by arguing that "*no nation which expects to be the leader of other nations can expect to stay behind in the race for space.*"² During his tenure, the number of NASA employees increased from 10,000 to 36,000 and its annual budget reached 47 billion USD, marking roughly 4.5% of the central budget.³ The American Apollo Mission was launched in 1961 with an initial budget of 531 million USD.⁴ Finally, Apollo 11 successfully landed on the moon in 1969.⁵ This was not only a landmark scientific achievement in human history but also a great strategic instrument symbolizing American scientific triumph in the context of the Cold War. Consequently, dominance in outer space and the race to surpass each other became a matter of pride for the USSR and the United States.

The military usage of outer space especially concentrated on how the space system and

satellites could contribute to nuclear deterrence, early warnings, nuclear command and control systems, and strategic stability. The official doctrine since the Dwight D. Eisenhower administration was guided by the Sanctuary School of thought, which argued that surveillance from outer space was an inevitable part of nuclear deterrence force (Mowthorpe, 2002; Berkowitz, 2011). Under the doctrine, the country deployed a U-2 High-altitude reconnaissance aircraft since 1956 in Soviet air space, which the USSR shot down in 1960 (Graham & Hansen, 2012, p. 36). In reaction, in the month following the U-2 incident, the US launched its first signal satellite GRAB-1 to collect Soviet air defence radar information (Clark, 2010).

The Reagan administration shifted its concern from the Sanctuary school to the High Ground School (high valued on space-based ballistic missile defence system) and ordered for the technological development of land and space-based ballistic missile defence (BMD) systems (Fukushima, 2013). The Carter administration developed the National Space Policy (NSP) in 1978 which stated that the reconnaissance satellites would provide support for the front-line troops.⁶ However, in reaction to US activities, the USSR developed Radar Ocean Reconnaissance Satellites (RORSATs) and Electronic Ocean Reconnaissance Satellite (EORSATs) that had posed significant challenges to US vessels.⁷ Under these conditions, space systems became a potential target of attack. Therefore, both countries developed and deployed ASAT weapons during the 1980s (Fukushima, 2013). In reaction to the USSR's development and deployment of ground-based ASAT in the 1980s (Nye & Schear, 1988, p. 11), the United States completed to five air-launched ASAT weapons test from 1984 to 1986 (Fukushima, 2013).

² Vartabedian R., Masunaga S. Could the Apollo 11 Moon Landing Be Duplicated Today? 'Lots of Luck with That' // Los Angeles Times. July 14, 2019. URL: <https://www.latimes.com/nation/la-na-could-apollo-11-be-repeated-20190714-story.html> (accessed: 31.01.2022).

³ Rodhan N. A. The Future of Meta-Geopolitical Competition in Outer Space // Italian Institute for International Political Studies (ISPI). July 20, 2019. URL: <https://www.ispionline.it/en/pubblicazione/future-meta-geopolitical-competition-outer-space-23531> (accessed: 31.01.2022).

⁴ Ibid.

⁵ Perrin O. Le programme Apollo, sur orbite de guerre froide // Le Temps. Juillet 15, 2019. URL: <https://www.letemps.ch/sciences/programme-apollo-orbite-guerre-froide> (accessed: 31.01.2022).

⁶ Presidential Directive/NSC-37 "National Space Policy" // The Aerospace Security Project at CSIS. May 11, 1978. URL: <https://aerospace.csis.org/wp-content/uploads/2019/02/PD-NSC-37-Carter-National-Space-Policy-11-May-1978-Redacted.pdf> (accessed: 31.01.2022).

⁷ The Soviet Space Challenge. Washington, D.C. : US Department of Defense, 1987. P. 11.

Post-Cold War Period

The fall of the Soviet Union considered the United States as a unitary actor in space operations. US continued to maintain technological superiority in outer space activities, for instance, Global Positioning System (GPS). During the Cold War period unlike the Soviet Union, the United States had multiple counter space programs, for example, Air-Launched Direct-Ascent Anti-Satellite (DA-ASAT) missile — ASM-135 — to counter the Soviet Union's co-orbital ASAT capability. Therefore, the United States briefly considered developing a new counter space capability (Weeden & Samson, 2018). However, all counter space efforts never materialized came into force due to different reasons like the budgetary problem, political factors, and focus on Global War on Terrorism following 9/11 attack (Weeden & Samson, 2018). In addition, Russia as a successor state of the Soviet Union and China as a rising power in space did not have the capability to deteriorate Washington's interest in outer space. But, following the end of the Cold War, the debate over the military engagements of outer space in wartime took a new meaning within the United States. However, the successful use of outer space technologies in the Gulf War in 1991, which is also called as First Space War,⁸ gained the importance of space activities. During the Operation Desert Storm around 60 military satellites were utilized to provide C4ISR support for the coalition forces.⁹ The "Control" school of thought, which implies that control of space will ensure free activity on Earth (White, 1958), has gained momentum in the US space administration.

After 2000s private funding along with government funding contributed to the US dominance in outer space technology. However, the economic and scientific rise of China

provided a tremendous opportunity for Beijing to take key positions in outer space. Over the last two decades, China has achieved significant developments in outer space capabilities across military, commercial and civil areas. Chinese Space program was established in the 1950s in reactions to the US and the Soviet Union's advancement in outer space for military purposes. PRC launched its first satellite in 1970 and sent astronaut into space in 2003. In 2007 China successfully tested its anti-satellite weapons by destroying its satellite in lower Earth orbit. This event encouraged other countries like India to develop anti-satellite weapons and the United States and Russia to restart their ASAT programs. For instance, the US Navy used Standard Missile (SM-3) to destroy old reconnaissance satellite in 2018¹⁰ and Russia also conducted ground-based anti-satellite weapons PL-19 Nudol.¹¹ In the following 2019 year, India also tested anti-satellite weapon.¹² Though there are immense potentials of non-military use of outer space, states are increasingly considering space from a traditional security perspective with aspirations of controlling space assets especially those highly linked to terrestrial military assets. Therefore the competition in space has been extensively focused on counter-space operations and capabilities. The growing rivalry and the lack of consistency of trust even among allies, such as the US and the European powers, are reflected in the development and use of diverse navigational systems.¹³ For instance, US's GPS,

¹⁰ Grego L. A History of Anti-Satellite Programs // Union of Concerned Scientists. January 2012. URL: https://www.ucsusa.org/sites/default/files/2019-09/a-history-of-ASAT-programs_lo-res.pdf (accessed: 31.01.2022).

¹¹ Chin J. Russia Conducted Seventh PL-19 ASAT Test in December 2018 // The CSIS Missile Defense Project. January 22, 2019. URL: <https://missilethreat.csis.org/russia-conducted-seventh-pl-19-asat-test-in-december-2018/> (accessed: 31.01.2022).

¹² Panda A. Exclusive: India Conducted a Failed Anti-Satellite Test in February 2019 // The Diplomat. March 30, 2019. URL: <https://thediplomat.com/2019/04/exclusive-india-conducted-a-failed-anti-satellite-test-in-february-2019/> (accessed: 31.01.2022).

¹³ Rodhan N. A. The Future of Meta-Geopolitical Competition in Outer Space // Italian Institute for International Political Studies (ISPI). July 20, 2019. URL:

⁸ Greenemeier L. GPS and the World's First "Space War" // Scientific American. February 8, 2016. URL: <https://www.scientificamerican.com/article/gps-and-the-world-s-first-space-war/> (accessed: 31.01.2022).

⁹ Fact Sheet: Joint Direct Attack Munition GBU-31/32/38 // U.S. Air Force. 2003. URL: <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104572/joint-direct-attack-munition-gbu-313238/> (accessed: 31.01.2022).

EU's GALILEO, Russian GLONASS, and the PRC's BeiDou are similar navigational satellite systems that illustrate the varying programs developing the technologies.

Importance of Space as a Strategic Domain

Human society is becoming increasingly dependent on space-based services and technologies mainly for communication services, defence and security, crisis management, transportation, and financial transactions. Space has become one of the rapidly expanding sectors in the world economy, worth 369 billion USD in 2020, estimated to rise to around 600 billion USD by 2030, and projected to be 1.053 trillion USD by 2040.¹⁴ It is playing a significant role in earth-based military activities, providing, for example, signal, navigational services, images, communication, and information services for military operations and most importantly in missile tracking. Although these services are considered auxiliary on the battlefield, they are playing a significant role even in advanced militaries such as the US. GPS, for instance, played a crucial role in the Gulf War for rapidly moving US-led coalition forces and identifying Iraqi military positions.¹⁵ Various studies and official statements suggest that the US military is overly dependent on space systems, so that its military operations are practically impossible without satellite communications and support.¹⁶

Consequently, the strategic importance of space lies not only in outer space activities, but also in military operations on land, in the air, at

sea and even in the cyberspace. Additionally, space systems are essential for the operationalization of nuclear forces. For example, dedicated early-warning satellites have been playing a crucial role in nuclear command and control system since the Cold War. Likewise, ballistic missile defence systems, missile targeting and delivery systems, intelligence, surveillance and reconnaissance (ISR) over other states' nuclear programs are also linked with space technology (Quintana, 2017). This feature of space technology is becoming increasingly significant in South Asia given the hostility between India and Pakistan, and India's consideration endeavours of a shift from its "first use" to "no-first-use" nuclear doctrine (Ali & Khalil, 2018). Thus, for the strategic balance and nuclear stability of the region, where India, Pakistan, and China possess nuclear arsenals and are strongly advancing their outer space capabilities, especially China and India, space technology is undoubtedly vital (Ali Khan & Imam, 2019). NATO Secretary General Jens Stoltenberg therefore identifies space as the next "operational domain" for military engagements.¹⁷ Finally, the combination of the heightened investment from the increasing number of small space powers like Luxemburg, South Korea and non-state actors like SpaceX, Virgin Galactic and the intensified competition between great powers like the US and China is making space a more strategic, contested and valuable domain.

United States Space Operations

The United States considers space power as vital to its national security. The US Strategic Command is responsible for conducting joint-space operations and the operational doctrine of space operations, highlighting "space control" and "space force applications."¹⁸ Additionally,

<https://www.ispionline.it/en/publicazione/future-meta-geopolitical-competition-outer-space-23531> (accessed: 31.01.2022).

¹⁴ Viens A. Visualized: The Race to Invest in the Space Economy // Visual Capitalist. November 21, 2019. URL: <https://www.visualcapitalist.com/visualized-the-race-to-invest-in-the-space-economy/> (accessed: 31.01.2022).

¹⁵ Greenemeier L. GPS and the World's First "Space War" // Scientific American. February 8, 2016. URL: <https://www.scientificamerican.com/article/gps-and-the-world-s-first-space-war/> (accessed: 31.01.2022).

¹⁶ Erwin S. Army Soldiers on the Front Lines of Space Wars // Space News. September 6, 2018. URL: <https://spacenews.com/army-soldiers-on-the-front-lines-of-space-wars/> (accessed: 31.01.2022).

¹⁷ Boffey D. NATO Leader Identifies Space as the Next 'Operational Domain' // The Guardian. November 20, 2019. URL: <https://www.theguardian.com/world/2019/nov/20/nato-identifies-space-as-next-operational-domain> (accessed: 31.01.2022).

¹⁸ Joint Publication 3-14 — Space Operations // Joint Chiefs of Staff. April 10, 2018. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14Ch1.pdf (accessed: 31.01.2022).

the US Air Force (USAF) has a specific document on space operations named “Doctrine of Counterspace Operations.”¹⁹ These documents and doctrines declare the US’s aspirations for dominance in space. The country has the largest number of satellites in outer space, which numbered 1308 in 2021.²⁰ As a result, it has the highest potential casualties in any potential space war, which determines the priority it gives to space defence. However, this overwhelming satellite capacity has given the US a significant advantage in ground-based combat. The development of counter-space capabilities and the conduct of space war exercises indicate that the country will respond aggressively if another space power undermines the US’s interest in space.

A growing challenge for the US is the rapid growth of China in space, which has replaced the Soviet Union. As in the South China Sea, China is expanding its presence in space, which is of concern to the Pentagon. Consequently, the US has developed kinetic and non-kinetic physical weapons to counteract space capabilities, which could permanently destroy satellites and ground-based support stations. Such weapons include DA-ASAT missile and co-orbital system.²¹ Although the Pentagon does not recognize co-orbital capabilities, it has the latent capability to develop in a short time if it wants.²² Pentagon technology chief Michael Griffin has announced his goal of deploying megawatt-class direct energy devices in space by 2020 to defend the US against adversaries’ long-range missiles.²³

¹⁹ Air Force Doctrine Publication 3-14 — Counterspace Operations // US Air Force. August 27, 2018. URL: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-14/AFDP-3-14-Counterspace-Ops.pdf (accessed: 31.01.2022).

²⁰ Salas E. B. Number of Satellites in Orbit by Country as of January 1, 2021 // Statista. July 21, 2021. URL: <https://www.statista.com/statistics/264472/number-of-satellites-in-orbit-by-operating-country/> (accessed: 31.01.2022).

²¹ Counterspace Capabilities // United Nations Institute for Disarmament Research. Geneva, 6—17 August, 2018. URL: <https://web.archive.org/web/20210415022613/https://unidir.org/files/medias/pdfs/counterspace-capabilities-background-eng-0-771.pdf> (accessed: 31.01.2022).

²² Ibid.

²³ Selinger M. DoD’s Griffin Eyes Using Directed Energy For Space-Based Missile // Defense Daily. April 17, 2018. URL: <https://www.defensedaily.com/>

The US has also developed a counter communication system and navigation warfare system. It has advanced cyber capabilities with potentials to destroy the enemy’s space system. Such dependence on the space system on the US’s part is viewed as a vulnerability by China.

Given China’s view of the over-dependence of the US military on its space system, Washington has taken steps to increase the resilience of its space system by implementing passive defences such as distribution, diversification, deception, protection, etc.²⁴ To respond to space challenges from the Chinese and Russians, the Trump administration recently established the US Space Force on 20 December 2019 to protect US and allied interests in space and provide space capabilities to the joint force.²⁵ China perceived this action as a “direct threat to outer space peace and security.”²⁶ In addition, NASA is also planning to send two astronauts to the South Pole of the Moon by 2024 and to establish an operation there substantially in the ensuing years.²⁷ Despite Trump’s stated intention to reduce NASA’s space budget, the organization continues to expand. For 2020 financial year (FY), 22.6 billion USD has been allocated for NASA, which is 5.3% more than FY 2019.²⁸

dods-griffin-eyes-using-directed-energy-space-based-missile-defense/pentagon/ (accessed: 31.01.2022).

²⁴ Lambakis S. Thinking about Space Deterrence and China // RealClearDefense. July 10, 2019. URL: https://www.realcleardefense.com/articles/2019/07/10/thinking_about_space_deterrence_and_china_114569.html (accessed: 31.01.2022).

²⁵ Morris E. U.S. Space Force Must Inspire the Next Generation of Military Space Professionals // Space News. January 6, 2020. URL: <https://spacenews.com/u-s-space-force-must-inspire-the-next-generation-of-military-space-professionals/> (accessed: 31.01.2022).

²⁶ Goodin E. China Attacks the Newly Formed U.S. Space Force as a ‘Direct Threat to Outer Space Peace and Security’ // Mail Online. December 23, 2019. URL: <https://www.dailymail.co.uk/news/article-7821261/China-attacks-US-Space-Force-threat-outer-space-peace.html> (accessed: 31.01.2022).

²⁷ Wall M. Can NASA Really Put Astronauts on the Moon in 2024? // Space.com. March 28, 2019. URL: <https://www.space.com/nasa-astronauts-moon-2024-feasibility.html> (accessed: 31.01.2022).

²⁸ Amadeo K. NASA Budget, Current Funding, History, and Economic Impact // The Balance. January 20, 2022. URL: <https://www.thebalance.com/nasa-budget-current-funding-and-history-3306321> (accessed: 31.01.2022).

Additionally, the Pentagon has requested 14.1 billion USD allocations in FY 2020 for the National Security Space Agencies.²⁹ Such extensive funding along with private funding always aids the country to retain a strong position in space research and technology. For instance, SpaceX, a private space company, is also playing a significant role in US space innovation. SpaceX is the first to develop a reusable launching system which reduces the cost of launching satellites.

Nevertheless, NASA has lost some of the unilateral and traditional prestige that it gained during the Apollo era. Due to the lack of a functional space shuttle, NASA is currently unable to fly astronauts anywhere in the world on its own. It has paid Russia more than 80 million USD for a seat to ride to the space station.³⁰ In 2014, NASA turned to SpaceX and Boeing to develop a 6.8 billion USD spacecraft that would allow the US to send astronauts from its soil again.³¹

Due to the delay of the US program, in 2020 NASA has completed negotiations with Roscosmos to purchase one additional seat on Russian Soyuz flight to the station.³² China is planning to establish a 200-tonne megawatt-level space-based solar power station by 2035 to capture solar energy.³³ This energy will be converted to microwave or lasers and then be sent back to the earth's surface for human consumption.³⁴ NASA abandoned a similar

project decades ago.³⁵ This project will allow China to sell clean energy at a lower price by undermining US energy firms.³⁶ Beijing provides commercial firms with launch services for its mobile intercontinental ballistic missiles at a nominal price, which is already 80% lower than the launch price in the US.³⁷ However, despite China's expressed willingness, since 2011 NASA has been forbidden to cooperate with it on space-related issues without congressional approval.³⁸

Russian Federation Space Operations

Outer space is considered by Russia as a strategic domain for increasing its military capabilities at the operational and defence level. At the same time, the weaponization of space is perceived as a threat to Russian assets in outer space. Therefore, Russia has taken symmetric and asymmetric action in outer space, enhancing counter space capabilities like ASAT test and at the same time, taking diplomatic initiatives in multilateral forums for controlling weaponization space (Jackson, 2018). Moreover, Moscow sees space activities as a way of achieving prestige and status as a space power as well as a great power (Jackson, 2018) and simultaneously as a source of revenue. Russia plans to take 10% of the global space market by 2030.³⁹

As a successor state of the former Soviet Union, Russia has a rich history and experience in outer space activities. The fall of the Soviet

²⁹ FY2020 National Security Space Budget Request: An Overview // Congressional Research Service. June 7, 2019. URL: <https://fas.org/sgp/crs/natsec/IF11244.pdf> (accessed: 31.01.2022).

³⁰ Davenport C. Another Front in the Tensions between the U.S. and China: Space // The Washington Post. July 26, 2019. URL: <https://www.washingtonpost.com/technology/2019/07/26/another-front-tensions-between-us-china-space/> (accessed: 31.01.2022).

³¹ Ibid.

³² NASA Completes Negotiations for Additional Soyuz Seat in Fall // NASA Blogs. May 12, 2020. URL: <https://blogs.nasa.gov/spacestation/2020/05/12/nasa-completes-negotiations-for-additional-soyuz-seat-in-fall/> (accessed: 31.01.2022).

³³ China to Build Space-Based Solar Power Station by 2035 // China Daily. February 12, 2019. URL: <https://www.chinadaily.com.cn/a/201912/02/WS5de47aa8a310cf3e3557b515.html> (accessed: 31.01.2022).

³⁴ Ibid.

³⁵ Rosenbaum E. China Plans a Solar Power Play in Space That NASA Abandoned Decades Ago // CNBC. March 17, 2019. URL: <https://www.cnbc.com/2019/03/15/china-plans-a-solar-power-play-in-space-that-nasa-abandoned-long-ago.html> (accessed: 31.01.2022).

³⁶ Autry G., Kwast S. America Is Losing the Second Space Race to China // Foreign Policy. August 22, 2019. URL: <https://foreignpolicy.com/2019/08/22/america-is-losing-the-second-space-race-to-china/> (accessed: 31.01.2022).

³⁷ Ibid.

³⁸ Wall M. China Eyes Robotic Outpost at the Moon's South Pole in Late 2020s // Space.com. July 18, 2019. URL: <https://www.space.com/china-moon-south-pole-research-station-2020s.html> (accessed: 31.01.2022).

³⁹ Zaborskiy V. Russia: From Space Programs to Space Strategy? // SpaceNews.com. May 2, 2012. URL: <https://spacenews.com/russia-space-programs-space-strategy/> (accessed: 31.01.2022).

Union and lack of funding in the space sector has allowed other competitors like the United States to be a unitary dominant player in outer space. After the decline in Russia's military capabilities, space was one of the few areas where Russia had international prestige, especially in human space flight. Even countries like the United States use the Russian RD-180 rocket engine in one of its main space launch systems Atlas V (Harrison et al., 2017). Russia, under the leadership of Vladimir Putin, reconstituted its space activities after 2000. Putin restarted several previously suspended counter space projects to restore its capability along with the military capability to counter US space dominance and missile defence systems. Russia has therefore developed various types of kinetic physical weapons, such as the A-235 PL-19 Nudol, which can attack a satellite in low Earth orbit.⁴⁰ Russia tested anti-satellite missile system at the end of 2018 from its mobile launch.⁴¹

During the Cold War, the Soviet Union developed various kinetic and non-kinetic physical counter-space systems. "Istrebitel Sputnikov" (IS) meaning "Satellite destroyer," and its modified version IS-MU were developed during the Cold War period, although its ground identifier segment continued to operate after the Cold War.⁴² The Soviet Union built the most powerful co-orbital ASAT — "Naryad", that was developed to threaten satellites in Geosynchronous Equatorial Orbit (GEO) and its launch system is still being used to launch satellites (Weeden & Samson, 2018). However, Russia is developing different types of modern ASAT weapons based on direct ascent technologies, that represent the shift from Soviet based technologies. Moreover, it is also

⁴⁰ Gertz B. Russia Flight Tests Anti-Satellite Missile // Washington Free Beacon. December 2, 2015. URL: <http://freebeacon.com/national-security/russia-conducts-successful-flight-test-of-anti-satellite-missile/> (accessed: 31.01.2022).

⁴¹ Panda A. Russia Conducts New Test of 'Nudol' Anti-Satellite System // The Diplomat. April 02, 2018. URL: <https://thediplomat.com/2018/04/russia-conducts-new-test-of-nudol-anti-satellite-system/> (accessed: 31.01.2022).

⁴² Zak A. IS Anti-Satellite System // Russian Space Web. January 27, 2021. URL: <http://www.russianspaceweb.com/is.html> (accessed: 31.01.2022).

developing different non-kinetic — nuclear, energy and laser-based — weapons and electronic systems for counter-space operations. Although Moscow is one of the main parties to the proposed "Treaty on Prevention of the Placement of Weapons in Outer Space, Threat or Use of Force against Outer Space Objects"⁴³ advocating the peaceful use of outer space, its counterspace operations and weapons development show contrary intentions. The United States refused this proposal and denied to sign it.⁴⁴

Russian missile defence systems are capable of reaching near space. For instance, Russian S-500 anti-ballistic missile air defence systems could be used for missile defence and ASAT purpose. In addition, Moscow has already completed the development of a laser-based ASAT weapons system like "Sokol Eshelon."⁴⁵ At the same time, Moscow started to advance its global navigational system GLONASS for military and civilian purposes and an upgraded military launching site at Plesetsk (Moltz, 2019). GLONASS has now improved its accuracy and reliability along with its ability to provide global coverage.⁴⁶

Russia's oil and gas revenues have enabled it to restart its space programme. French expert Bertrand de Montluc (2010) described this rise as a 'resurgence' of Russia in the outer space

⁴³ Proposed Prevention of an Arms Race in Space (PAROS) Treaty // Nuclear Threat Initiative. 2020. URL: <http://www.nti.org/learn/treaties-and-regimes/proposed-prevention-arms-race-space-paros-treaty/> (accessed: 10.03.2021).

⁴⁴ Foust J. U.S. Dismisses Space Weapons Treaty Proposal as "Fundamentally Flawed" // Space News. September 11, 2014. URL: <https://spacenews.com/41842us-dismisses-space-weapons-treaty-proposal-as-fundamentally-flawed/> (accessed: 31.01.2022).

⁴⁵ Cenciotti D. Russia Has Completed Ground Tests of Its High-Energy Airborne Combat Laser System // The Aviationist. October 5, 2016. URL: <https://theaviationist.com/2016/10/05/russia-has-completed-ground-tests-of-its-high-energy-airborne-combat-laser-system/> (accessed: 31.01.2022).

⁴⁶ Urlichich Y., Subbotin V., Stupak G., Dvorkin V., Povalyaev A., Karutin S., Bakitko R. GLONASS Modernization // GPS World. November 1, 2011. URL: <http://gpsworld.com/glonass-modernization-12232/> (accessed: 31.01.2022).

domain. However, he also argued that the Russian long-term plan for space is quite unclear. Despite lagging behind in some civilian space activities, Moscow is still the dominant player in military space and has extensive experience in counter-space operations. Russia established “the Russian Aerospace Force” in 2015, which composed of the Air Force and Aerospace Defence Force (Myers, 2018). This space force aims to monitor and identify space objects and threats, prevent counter space activities, launch and control satellites for the military — especially for countering NATO threat⁴⁷ — and civilian purposes. On the other hand, in the civilian space programme, the Soyuz space capsule still provides Moscow with a leadership position to reach the ISS. Due to the delay in building a NASA spacecraft, the U.S. and other countries still depend on Russia to send their astronauts to the ISS. However, in 2019, NASA planned to deploy its commercial crews by the summer of 2022.⁴⁸ As of spring 2022, two operational flights were carried out, which took astronauts to the ISS, as part of the NASA Commercial Crew Program.⁴⁹

Russia began its start-up sector by founding the Skolkovo Innovation Center (Moltz, 2019). Moreover, several small firms have emerged in the start-up sector with the help of public funding (McClintock, 2017), but their activities fail to flourish because of the opposition of the state sector in terms of Russian preferences for traditional technocracy (Moltz, 2019). To reduce its dependence on Baikonur, for which Russia pays Kazakhstan 115 million USD annually,⁵⁰

⁴⁷ Bodner M. Russia Merges AF with Missile Defense, Space Commands // *Defense News*. August 8, 2015. URL: <https://www.defensenews.com/2015/08/08/russia-merges-af-with-missile-defense-space-commands/> (accessed: 31.01.2022).

⁴⁸ Report No. IG-20-005 “NASA’s Management of Crew Transportation to the International Space Station” // NASA Office of Inspector General Office of Audits. November 14, 2019. URL: <https://oig.nasa.gov/docs/IG-20-005.pdf> (accessed: 31.01.2022).

⁴⁹ SpaceX’s Crew-3 Astronaut Mission Will Return to Earth Early Friday // *Space.com*. May 3, 2022. URL: <https://www.space.com/spacex-crew3-mission-return-to-earth-friday> (accessed: 31.01.2022).

⁵⁰ “Kazakhstan Finally Ratifies Baikonur Rental Deal with Russia” // *Space Daily*. April 12, 2010. URL:

Moscow built the Vostochny Cosmodrome on Russian territory in the Far East. Putin announced that this new launch site would be built for civilian purposes.

After 2000, the Russian space programme was growing well again. Compared to the 1990s, Roscosmos received a large budget from the government. In 2013, Roscosmos got 5.6 billion USD for the development of space tourism and the Angara rocket family.⁵¹ After that, the space budget was reduced. In 2016, the Russian government approved a 10-year space programme (Federal Space Programme 2016—2025) worth 20.5 billion USD.⁵² However, the draft budget for this programme was 56.4 billion USD.⁵³ Due to falling oil prices on the international market and Western sanctions against Russia, Moscow has been forced to cut its budget. The Russian space budget was supposed to increase slightly in 2020, but Roscosmos received only 2.77 billion USD for that year.⁵⁴ Igor Komarov, former head of Roscosmos, declared that by 2025 Russian orbital assets will grow from 49 to 73 operational spacecraft and communication satellites will grow from 32 to 41, with the moon landing remaining a strategic goal, tentatively scheduled for 2030.⁵⁵

The Soviet legacy has given an advantage to today’s Russia. However, Moscow has failed to maintain the progress it made during the Soviet

https://www.spacedaily.com/reports/Kazakhstan_Finally_Ratifies_Baikonur_Rental_Deal_With_Russia_999.html (accessed: 31.01.2022).

⁵¹ McCarthy N. Infographic: The World Trails NASA in Space Exploration Expenditure // *Statista*. October 14, 2014. URL: <https://www.statista.com/chart/2824/space-exploration-expenditure/> (accessed: 31.01.2022).

⁵² Zak A. Russia Approves Its 10-year Space Strategy // *Planetary Society*. March 23, 2016. URL: <https://www.planetary.org/articles/0323-russia-space-budget> (accessed: 31.01.2022).

⁵³ *Ibid.*

⁵⁴ In Roscosmos Compared Their Budget and NASA [В Роскосмосе сравнили свой бюджет и NASA] // *TASS*. February 11, 2020. URL: <https://tass.ru/ekonomika/7734535> (accessed: 31.01.2022). (In Russian).

⁵⁵ Zak A. Russia Approves Its 10-year Space Strategy // *Planetary Society*. March 23, 2016. URL: <https://www.planetary.org/articles/0323-russia-space-budget> (accessed: 31.01.2022).

period. One of the major problems in the modern Russian space industry is the misappropriation of Roscosmos funds.⁵⁶ Most of the current generations satellite components are coming from the United States (Moltz, 2019). Due to the western sanction, Russia is unable to get the standard equipment for the satellite programme. Therefore, Moscow depends on its domestic or substandard products from other countries. Russia may be capable of developing all capabilities, but it will take time and it needs funding to make these efforts successful. The rise of various private space companies in the US has created challenges for the Russian space sector. The Russians are offering cheap prices for the satellite launching where Roscosmos are unable to offer a lower price. On the other hand, Roscosmos itself actively works to block the emergence of private space companies in Russia.

Space Operations of the People's Republic of China

The Chinese military White Paper identifies space as “a commanding height in the international strategic competition.”⁵⁷ China perceives space power as a prerequisite for enhancing its national strength. Its ambition is to become a global space power like the US and found a space industry like the US, Russia and EU. China takes a comprehensive approach to space that will give Beijing military, economic and political advantages at the international level.⁵⁸

China's strategic culture views space and military programs as the same entity, revealing a

clear preference for developing strategic hard power use in space.⁵⁹ China considers the US and Indian space activities as significant threats. The country is afraid that outer space can be affected by any future conflict. China's successful ASAT test in 2007 reflects this concern (Tellis, 2007). However, China has expressed a long-standing opposition towards the weaponization of outer space (Shen, 2011). China shares a long land border with India — a country with whom Beijing engaged in a border conflict in 1962. The military stand-off between the countries in Doklam plateau in 2017 also nearly led to war.⁶⁰ Both parties have military satellites for surveillance and reconnaissance and monitoring their adversaries' borders.

The US naval presence in the South China Sea is also a substantial threat to China, and is highly linked to the satellite system. Moreover, the Indian Navy has been developing military communications satellite GSAT-7s since 2013, which provide real-time communications among its warships submarine, aircraft, and land system. Therefore, China has developed Anti-Access/Area Denial (A2/AD) weapons which are a major threat against any sea-borne force. However, A2/AD requires an advanced level of surveillance, intelligence, reconnaissance, advance targeting with naval, air, and cyber and missile defence capability. In modern warfare, such capabilities require significant tracking and C4ISR capacities which are linked to advanced space capability and satellite infrastructure. Moreover, substantial tracking is also needed for implementing A2/AD which also requires “high-quality real-time satellite imagery and target locating data and fusion, as well as reliable indigenous satellite positioning, navigation, and timing (PNT)” (Erickson, 2013).

⁵⁶ Cowing K. Roscosmos Plans to Keep ISS Flying with Imaginary Money // NASA Watch. March 25, 2019. URL: <http://nasawatch.com/archives/2019/03/roscosmos-plans.html> (accessed: 31.01.2022).

⁵⁷ Chinese Defence White Paper “China's Military Strategy” // The State Council of People's Republic of China. May 27, 2015. URL: http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm (accessed: 31.01.2022).

⁵⁸ Pollpeter K., Anderson E., Wilson J., Yang F. China Dream, Space Dream: China's Progress in Space Technologies and Implications for the United States // US — China Economic and Security Review Commission. February 3, 2015. URL: https://www.uscc.gov/sites/default/files/Research/China%20Dream%20Space%20Dream_Report.pdf (accessed: 31.01.2022).

⁵⁹ Rodhan N. A. The Future of Meta-Geopolitical Competition in Outer Space // Italian Institute for International Political Studies (ISPI). July 20, 2019. URL: <https://www.ispionline.it/en/publicazione/future-meta-geopolitical-competition-outer-space-23531> (accessed: 31.01.2022).

⁶⁰ Marcus J. China — India Border Tension: Satellite Imagery Shows Doklam Plateau Build-Up // BBC News. January 26, 2018. URL: <https://www.bbc.com/news/world-asia-china-42834609> (accessed: 31.01.2022).

Consequently, China is exceptionally increasing its number of satellites. China now has 356 satellites, but in 2000 there were only 10.⁶¹ In comparison, the US and Russia have 1308 and 167 respectively, China has already surpassed Russia.⁶² It is also reported that China will send more than 40 satellites in 2020.⁶³ Like the US, China has also made significant progress in the development of the electronic and cyber capabilities of kinetic and non-kinetic physical.⁶⁴ Beijing is also developing direct energy weapons⁶⁵ and planning to deploy them by 2020⁶⁶ in the People's Liberation Army Navy.⁶⁷ It was reported that Beijing tried to attack a US satellite through laser weapons.⁶⁸ The Chinese military was also suspected of launching cyber-attack on US satellites,⁶⁹ although China denied

such claims.⁷⁰ Space-based weapons will provide China not only protection from its enemies, but also the ability to deny its enemies. China has deployed satellites with different range of capabilities, for example, electro-optical (EO), electro-reconnaissance (ELINT), and synthetic aperture radar (SAR) (Cordesman, 2016).

Space capability is highly important for appropriate missile guidance. An “unforgettable humiliation” experienced by the Chinese People's Liberation Army during the 1995—1996 Taiwan Strait Crisis pushed Beijing to develop its navigational system, BeiDou. During that crisis, the PLA launched missile testing operations near Taiwan. In the middle of those tests, the PLA was unable to track several of its launched missiles. The PLA argued that this happened due to the interference in GPS which is owned by the US. A retired Chinese colonel stressed that “it was a great shame for the PLA... an unforgettable humiliation. That's how we made up our mind to develop our own global (satellite) navigation and positioning system, no matter how huge the cost, BeiDou is a must for us. We learned it the hard way.”⁷¹

Therefore, after spending a huge amount of time and money, China is developing its own version of the global positioning system, BeiDou (Karimi, 2016). By 2020, BeiDou—3, consisting of 35 satellites, has become fully operational. Upon completion, it will provide navigational service on the level of the US GPS, Russian GLONASS, and European Galileo systems. Since most of the missiles use some sort of GPS or similar type of technology for targeting, BeiDou will be a remarkable achievement for China in space competition with other great powers, especially with the United States. BeiDou will challenge US GPS because it will be

⁶¹ Salas E. B. Number of Satellites in Orbit by Country as of January 1, 2021 // Statista. July 21, 2021. URL: <https://www.statista.com/statistics/264472/number-of-satellites-in-orbit-by-operating-country/> (accessed: 31.01.2022).

⁶² Ibid.

⁶³ Howell E. China Kicks Off 2020 with Mystery Satellite Launch: Report // Space.com. January 11, 2020. URL: <https://www.space.com/china-mystery-satellite-tjs-2-launch-success.html> (accessed: 31.01.2022).

⁶⁴ Counterspace Capabilities // United Nations Institute for Disarmament Research. Geneva, 6—17 August, 2018. URL: <https://web.archive.org/web/20210415022613/https://unidir.org/files/medias/pdfs/counterspace-capabilities-backgroundunder-eng-0-771.pdf> (accessed: 31.01.2022).

⁶⁵ Fisher Jr. R.D. China's Progress with Directed Energy Weapons. Testimony before US — China Economic and Security Review Commission Hearing // US — China Economic and Security Review Commission. February 23, 2017. URL: https://www.uscc.gov/sites/default/files/Fisher_Combined.pdf (accessed: 31.01.2022).

⁶⁶ Keller J. China May Deploy Anti-Satellite Laser Weapons Next Year Able to Destroy U.S. Military Satellites // Military & Aerospace Electronics. February 18, 2019. URL: <https://www.militaryaerospace.com/trusted-computing/article/16711585/china-may-deploy-antisatellite-laser-weapons-next-year-able-to-destroy-us-military-satellites> (accessed: 31.01.2022).

⁶⁷ Malyasov D. China Discloses New Directed-Energy Weapon Development // Defence Blog. April 4, 2019. URL: <https://defence-blog.com/china-discloses-new-directed-energy-weapon-development/> (accessed: 31.01.2022).

⁶⁸ Muradian V. China Tried to Blind U.S. Sats with Laser // AR15.COM. September 22, 2006. URL: https://www.ar15.com/forums/general/China_Tried_To_Blind_U_S_Sats_With_Laser/5-501978/ (accessed: 16.01.2022).

⁶⁹ Capaccio A., Bliss J. Chinese Military Suspected in Hacker Attacks on US Satellites // Bloomberg. October 27,

2011. URL: <https://www.bloomberg.com/news/articles/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites> (accessed: 31.01.2022).

⁷⁰ Wolf J. China Key Suspect in U.S. Satellite Hacks: Commission // Reuters. October 28, 2011. URL: <https://www.reuters.com/article/us-china-usa-satellite-idUSTRE79R4O320111028> (accessed: 31.01.2022).

⁷¹ Chan M. ‘Unforgettable Humiliation’ Led to Development of GPS Equivalent // South China Morning Post. November 13, 2009. URL: <https://www.scmp.com/article/698161/unforgettable-humiliation-led-development-gps-equivalent> (accessed: 31.01.2022).

accurate within millimeters.⁷² China also proclaimed to have made a historic landing, as the first country, of the robotic probe “Chang’e 4” on the most remote side of the Moon.⁷³ However, China tried to produce cotton on the soil of the Moon and failed.⁷⁴ China is planning to establish a robotic station on the South Pole (possible source of water) of the Moon by the end of the 2020s for the same reason as NASA.

However, China, like the US, has faced some problems. Its new rocket, Long March 5, failed shortly after liftoff. China’s Mars, Moon, and Space Station missions were reportedly delayed due to the failure of this new rocket, which is the main launching vehicle for China.⁷⁵ Moreover, China does not have longstanding technological experience and heritage like the US in space technology. Additionally, China’s budget for space has surpassed that of Russia, but it is still far behind the US in terms of military budget. In 2018, China and Russia spent about 5.8 billion USD and 4.2 billion USD respectively, whereas the US spent about 40.9 billion USD.⁷⁶ Unlike the US, China does not have strong private space sector for funding and research like SpaceX and the Sierra Nevada Corporation (Tronchetti, 2020).

Implications of Outer Space Competition

During the Cold War outer space rivalry had brought some significant civilian benefits along

⁷² Miranda E. BeiDou Navigation Satellite System: China’s More Accurate Version of GPS Nears Completion // Yibada. June 17, 2016. URL: <http://en.yibada.com/articles/132467/20160617/beidou-navigation-satellite-system-chinas-more-accurate-version-of-gps-nears-completion.htm> (accessed: 31.01.2022).

⁷³ Held A. China Tried to Grow Cotton on the Moon, but It Didn’t Work // KPBS. January 17, 2019. URL: <https://www.kpbs.org/news/2019/jan/17/plant-china-mooned-over-dies-couldnt-cotton-to/> (accessed: 31.01.2022).

⁷⁴ Ibid.

⁷⁵ Jones A. China’s Moon, Mars and Space Station Missions May Be Facing Delays // Space.com. June 24, 2019. URL: <https://www.space.com/china-moon-mars-space-station-missions-delays.html> (accessed: 31.01.2022).

⁷⁶ Seminari S. Global Government Space Budgets Continue Multiyear Rebound // Space News. November 24, 2019. URL: <https://spacenews.com/op-ed-global-government-space-budgets-continues-multiyear-rebound/> (accessed: 31.01.2022).

with military ones. Thus, the current and future outer space competition will also benefit the world through commercial and technological development. Due to such competitiveness, states will thrive for both invention and innovation for better telecommunication system, global positioning systems, mining, spinoff technology, human presence in off-planet, financial system, and as a potential source of energy. However, interruption to these services can seriously affect the functioning of modern life whilst bring huge economic loss, which can affect a state’s military competence. At the same time, the growing potential for mining valuable resources in space raised the possibility of even greater economic value and competition in the space domain.⁷⁷ Conversely, competition in outer space among great powers like Washington, Moscow and Beijing carries a risk for all parties. Mutual destruction of three great powers will be possible not only for the earthly nuclear war but also as a result of a missile launch from outer space.⁷⁸

Moreover, the possible militarization of outer space could threaten the peaceful purpose of outer space activities. Additionally, due to uncontrolled space activities, the most important concern at present is the increasing amount of space debris that can threaten human life on earth. China’s 2007 ASAT test created more than 3,000 pieces of debris in lower Earth orbit, some 800 km above the Earth.⁷⁹ The accidental collision between two satellites — the American Iridium Satellite and the Russian Cosmos 2251 — produced 1200 pieces of debris (Jaramillo, 2011). NASA identified 400 pieces of space debris from the event of Indian ASAT test

⁷⁷ Black J. Our Reliance on Space Tech Means We Should Prepare for the Worst // Defense News. March 12, 2018. URL: <https://www.defensenews.com/space/2018/03/12/our-reliance-on-space-tech-means-we-should-prepare-for-the-worst/> (accessed: 31.01.2022).

⁷⁸ Borroz N. The Risks and Rewards of Growing US — China Space Rivalry // The Diplomat/ September 13, 2019. URL: <https://thediplomat.com/2019/09/the-risks-and-rewards-of-growing-us-china-space-rivalry/> (accessed: 16.01.2022).

⁷⁹ Vasani H. How China Is Weaponizing Outer Space // The Diplomat. January 19, 2017. URL: <https://thediplomat.com/2017/01/how-china-is-weaponizing-outer-space/> (accessed: 31.01.2022).

in 2019.⁸⁰ However, since debris can also be produced by natural reasons, there is a possibility of inter-state cooperation on this issue.

Finally, the expansion of outer space activities either for military or civilian purpose will continue in the near future and will undoubtedly bring tremendous achievements. The USAF Space Commander, Major General Shaw, reflects this by saying, “we don’t know exactly when the human sphere of influence will expand to the Moon and Mars, but we do know it will happen.”⁸¹

Conclusion

Space is a relatively new strategic domain. Strategists tend to apply theories and experiences gained in terrestrial conflicts, although all theories are not applicable in space because of its nature (Mendenhall, 2018). Competition in space has been around since the very beginning, when the field came into existence. It started with the USSR and the US. Nowadays, multiple players are increasingly engaged in the process. Nevertheless, the US, Russia, and China are the major actors in the current scenario.

⁸⁰ Lewin S. India’s Anti-Satellite Test Created Dangerous Debris, NASA Chief Says // Space.com. April 2, 2019. URL: <https://www.space.com/nasa-chief-condemns-india-anti-satellite-test.html> (accessed: 31.01.2022).

⁸¹ The Future of Space 2060 and Implications for U.S. Strategy: Report on the Space Futures Workshop // Politico. September 5, 2019. URL: <https://www.politico.com/f/?id=0000016d-0513-d6ab-a97f-4f93520b0001> (accessed: 12.01. 2022).

The strategic importance of space is increasing gradually because of its dual-use nature. Considering such importance, space control by great powers is likely to become a prime issue. Based on the operational doctrines of the US, China and Russia, their rivalry is likely to continue in the coming days. China will take significant steps to catch up, both civilian and military, as it is a newcomer to this area compared to the US. On the other hand, Russian effort in outer space is not a new phenomenon. However, the various moves by Beijing and Moscow are seen as a threat by Washington. Similarly, China and Russia also perceive the US as the biggest threat to their interests. Chinese strategists believe that to counter the conventional superiority of the US, Beijing needs the ability to strike at Washington’s “Achilles heel”: over-dependence on US satellites. Hence, the US is also planning to strengthen its traditional space system with modern technology and new policy. As a result, outer space will play a dominant role on the battlefield of the 21st century. We can therefore expect the great powers to weaponise outer space in the coming days. In addition, the uniqueness of outer space in terms of orbital paths and radiation, the counter space capabilities by space powers with kinetic and non-kinetic weapons make space highly dangerous. However, historical experience shows that this space competition between the great powers is likely to yield significant benefits for humanity.

Received / Поступила в редакцию: 09.04.2021

Revised / Доработана после рецензирования: 12.12.2021

Accepted / Принята к публикации: 18.04.2022

References / Библиографический список

- Ali Khan, S., & Imam, I. (2019). Outer space and strategic stability in South Asia. *Astropolitics*, 17(1), 70—76. <https://doi.org/10.1080/14777622.2019.1578936>
- Ali, S., & Khalil, T. (2018). Debating potential doctrinal changes in India’s nuclear ambitions. *IPRI Journal*, 18(2), 53—77. <https://doi.org/10.31945/iprij.180203>
- Berkowitz, B. (2011). *The National Reconnaissance Office at 50 years: A brief history*. Chantilly, Virginia: Center for the Study of National Reconnaissance.
- Clark, R. M. (2010). *The technical collection of intelligence*. Washington, DC: SAGE Publications.
- Cordesman, A. H. (2016). China space strategy and developments. *CSIS Report*, 1—34. Retrieved from <https://www.csis.org/analysis/china-space-strategy-and-developments>
- Erickson, A. S. (2013). *Chinese anti-ship ballistic missile (ASBM) development: Drivers, trajectories, and strategic implications*. Washington, DC: Jamestown Foundation/Brookings Institution Press.

- Fukushima, Y. (2013). Debates over the military value of outer space in the past, present and the future: Drawing on space power theory in the US. *NIDS Journal of Defense and Security*, (14), 35—48.
- Graham Jr., T., & Hansen, K. A. (2012). *Spy satellites and other intelligence technologies that changed history*. Washington, DC: University of Washington Press.
- Harrison, T., Hunter, A., Johnson, K., Roberts, T. G., & Linck, E. (2017). Beyond the RD-180. *Report of the CSIS Aerospace Security Project*, 1—48. Retrieved from <https://aerospace.csis.org/beyond-rd-180/>
- Jackson, N. J. (2018). Outer space in Russia's security strategy. *Simons Working Paper in Security and Development*, (64), 1—22. Retrieved from <https://summit.sfu.ca/item/18164>
- Jaramillo, C. (Ed.). (2011). *Space security 2011*. Kitchener, Ontario: Pandora Press.
- Karimi, H. A. (2016). *Advanced location-based technologies and services*. CRC Press.
- McClintock, B. (2017). The Russian space sector: Adaptation, retrenchment, and stagnation. *Space and Defense*, 10(7), 3—8.
- Mendenhall, E. (2018). Treating outer space like a place: A case for rejecting other domain analogies. *Astropolitics*, 16(2), 97—118. <https://doi.org/10.1080/14777622.2018.1484650>
- Moltz, J. C. (2019). The changing dynamics of twenty-first-century space power. *Journal of Strategic Security*, 12(1), 15—43. <https://doi.org/10.5038/1944-0472.12.1.1729>
- Montluc, B. de. (2010). Russia's resurgence: Prospects for space policy and international cooperation. *Space Policy*, 26(1), 15—24. <https://doi.org/10.1016/j.spacepol.2009.12.002>
- Mowthorpe, M. (2002). US Military space policy 1945—92. *Space Policy*, 18(1), 25—36. [https://doi.org/10.1016/S0265-9646\(01\)00055-8](https://doi.org/10.1016/S0265-9646(01)00055-8)
- Myers, N. (2018). The Russian aerospace force. *Security Forum*, 2(1), 91—103. https://doi.org/10.26410/SF_1/18/8
- Nye, J. S., & Schear, J. A. (1988). *Seeking stability in space: Anti-satellite weapons and the evolving space regime*. Lanham, MD, London: University Press of America for Aspen Strategy Group.
- Quintana, E. (2017). The new space age: Questions for defence and security. *The RUSI Journal*, 162(3), 88—109. <https://doi.org/10.1080/03071847.2017.1352377>
- Shen, D. (2011). A collaborative China — US approach to space security. *Asian Perspective*, 35(4), 521—536. <https://doi.org/10.1353/apr.2011.0022>
- Tellis, A. J. (2007). China's military space strategy. *Survival*, 49(3), 41—72. <https://doi.org/10.1080/00396330701564752>
- Tronchetti, F. (2020). *The privatization of Chinese space activities: A legal and regulatory perspective*. *Journal of Space Law*, 44(2), 565—590.
- Weeden B., & Samson, V. (Eds.). (2018). Global counterspace capabilities: An open source assessment. *Report of Secure World Foundation*, 1—148. Retrieved from http://swfound.org/media/206118/swf_global_counterspace_april2018.pdf
- White, T. D. (1958). Space control and national security. *Air Force Magazine*, 41(4), 80—83.

About the author: *Islam Md Badrul* — Lecturer, Department of International Relations, Bangabandhu Sheikh Mujibur Rahman Science and Technology University; ORCID: 0000-0002-2990-3663; e-mail: badrul.islam@bsmrstu.edu.bd

Сведения об авторе: *Ислам Мд Бадрул* — преподаватель кафедры международных отношений Научно-технического университета имени Бангабандху Шейха Муджибура Рахмана; ORCID: 0000-0002-2990-3663; e-mail: badrul.islam@bsmrstu.edu.bd



DOI: 10.22363/2313-0660-2022-22-2-411-421

Научная статья / Research article

Глобальная террористическая угроза в Сахеле и истоки терроризма в Буркина-Фасо

Л.М. Исаев^{1, 2, 3}  , А.В. Коротаев^{1, 2, 3} , Д.А. Бобарькина⁴ 

¹Национальный исследовательский университет «Высшая школа экономики», Москва, Российская Федерация

²Институт Африки РАН, Москва, Российская Федерация

³Российский университет дружбы народов, Москва, Российская Федерация

⁴Санкт-Петербургская школа социальных наук и востоковедения Национального исследовательского университета «Высшая школа экономики», Санкт-Петербург, Российская Федерация

 lisaev@hse.ru

Аннотация. В статье рассматриваются причины роста террористической активности в Буркина-Фасо после революции 2014 г. Регион Сахель на протяжении десятилетий являлся одним из наиболее нестабильных в Африке и африканской зоне нестабильности. Однако в 2010-е гг. Сахель испытал на себе сильнейший рост террористической активности: к 2015 г. количество терактов здесь выросло более чем в семь раз по сравнению с 2010 г. В то же время динамика террористической активности в Буркина-Фасо имела свои особенности по сравнению с остальными странами Сахеля. Рост терроризма в этой стране во многом стал следствием свержения режима Б. Компаоре. Новые власти оказались неспособны поддерживать безопасность на прежнем уровне. Объяснением этому могут служить, с одной стороны, устойчивые договоренности, которые сложились между Компаоре и террористическими структурами. Его отставка разрушила все неформальные связи и договоренности, которые режим налаживал с региональными джихадистскими организациями, развязав им руки для достаточно быстрого и легкого проникновения в Буркина-Фасо. С другой стороны, важную роль сыграл роспуск Президентской гвардии (именно эта структура в значительной степени отвечала за борьбу с терроризмом) после неудачной попытки военного переворота в сентябре 2015 г. Новое руководство лишило страну защиты, которую они имели против джихадистских организаций, готовых проникнуть через границу в Буркина-Фасо. В результате после 2015 г. весьма благополучная с точки зрения терроризма страна столкнулась с беспрецедентным ростом террористической активности.

Ключевые слова: черная весна, Буркина-Фасо, Сахель, терроризм, нестабильность

Благодарности: Статья подготовлена в рамках гранта РФФИ 19-18-00155 «Исламистский экстремизм в контексте международной безопасности: угрозы России и возможности противодействия».

© Исаев Л.М., Коротаев А.В., Бобарькина Д.А., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

Для цитирования: Исаев Л. М., Коротаев А. В., Бобарыкина Д. А. Глобальная террористическая угроза в Сахеле и истоки терроризма в Буркина-Фасо // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 411—421. <https://doi.org/10.22363/2313-0660-2022-22-2-411-421>

The Global Terrorist Threat in the Sahel and the Origins of Terrorism in Burkina Faso

Leonid M. Issaev^{1, 2, 3}  , Andrey V. Korotayev^{1, 2, 3} , Daria A. Bobarykina⁴ 

¹HSE University, Moscow, Russian Federation

²Institute for African Studies of the Russian Academy of Sciences, Moscow, Russian Federation

³Peoples' Friendship University of Russia (RUDN University), Moscow, Russian Federation

⁴Saint-Petersburg School of Social Sciences and Area Studies under HSE University, Saint-Petersburg, Russian Federation

 lisaev@hse.ru

Abstract. The article examines the reasons for the increasing terrorist activity in Burkina Faso after the revolution in 2014. For decades, the Sahel has been one of the most unstable regions in Africa and the Afrasian zone of instability. However, in the 2010s the Sahel has experienced a dramatic increase in terrorist activity: by 2015, the number of terrorist attacks there increased more than seven times compared to 2010. At the same time, the dynamics of terrorist activity in Burkina Faso had its specific characteristics compared to the rest of the Sahel. The growth of terrorism in this country was largely a consequence of the overthrow of the B. Compaoré regime. The new authorities were unable to maintain security at the same level. This can be explained, on the one hand, by the stable agreements that had been settled between Compaoré and terrorist structures. His resignation destroyed all the informal ties and agreements that the regime had established with regional jihadist organizations, freeing their hands to infiltrate Burkina Faso quickly and easily. On the other hand, the dissolution of the Regiment of Presidential Security (precisely the structure largely responsible for the fight against terrorism) after the failed military coup attempt of September 2015 played an important role. The new leadership stripped the country of the protection they had against jihadist organizations poised to infiltrate across the border into Burkina Faso. As a result, after 2015, a very safe country in terms of terrorism faced an unprecedented increase in terrorist activity.

Key words: Black Spring, Burkina-Faso, Sahel, terrorism, instability

Acknowledgements: The article was prepared within the framework of the Russian Science Foundation grant 19-18-00155 “Islamist extremism in the context of international security: threats to Russia and opportunities for counteraction”.

For citation: Issaev, L. M., Korotayev, A. V., & Bobarykina, D. A. (2022). The global terrorist threat in the Sahel and the origins of terrorism in Burkina Faso. *Vestnik RUDN. International Relations*, 22(2), 411—421. <https://doi.org/10.22363/2313-0660-2022-22-2-411-421>

Введение

Терроризм является источником социально-политической нестабильности во всей африканской зоне нестабильности¹. Наши предыдущие исследования показали, что «арабская весна» создала благоприятные условия для распространения ближневосточного терроризма за пределы арабского мира (Issaev, Fain & Korotayev, 2021; Исаев и др.,

2020; Коротаев и др., 2019). Одним из регионов, в котором «арабская весна» послужила триггером роста террористической активности, стал Сахель².

Как пишет Дж. Дентис, «Сахель — это источник многочисленных кризисов, в которых многочисленные движущие террористические силы создали условия для роста новых

¹ Подробнее об африканской зоне нестабильности см.: (Коротаев и др., 2015).

² Под странами Сахеля здесь и далее понимается группа G5 Сахель, в которую входят Буркина-Фасо, Мали, Чад, Мавритания и Нигер.

угроз в регионе» (Dentice, 2018, p. 1). Отмечается, что «регион характеризуется целым рядом проблем, в том числе нестабильностью внутри государств, слабыми институтами, отсутствием социальной справедливости, безработицей и бедностью» (Danjibo, 2013, pp. 18—19).

Многие работы, посвященные терроризму в Сахеле, в качестве причин этого явления выделяют сложную внутривластную ситуацию, а также фактор внешнего влияния (Dentice, 2018, p. 1). Как отмечают И.Н. Ньядера и Х. МассAUD (Nyadera & Massaoud, 2019), в объяснении насилия в Сахеле важное место занимает теория неуправляемого пространства и конфликтов, согласно которой отсутствие эффективной деятельности со стороны правительства со временем может привести к дезинтеграции и политической дестабилизации. В связи с этим население такого государства становится уязвимым, что позволяет вооруженным группам и террористическим организациям заручиться поддержкой людей, которые чувствуют себя изолированными в стране. Таким образом, годы неэффективного управления государствами Сахеля создали в них очаги неуправляемых территорий, которые эксплуатируются вооруженными группами (Nyadera & Massaoud, 2019).

И. Атия в свою очередь отмечает, что терроризм и организованная преступность в странах Сахеля появились в результате долгой колониальной власти в этих странах (Attiya, 2017, p. 60). Борьба местного населения за независимость вела к восстаниям, которые впоследствии приводили к неустойчивости создаваемых независимых государств. Ввиду внутривластной нестабильности в отдельных странах зоны Сахеля часто вспыхивали революции и гражданские войны, что приводило к активизации террористической деятельности. Таким образом, терроризм в этих странах представляет собой особую форму насилия и истощения государства (Attiya, 2017, p. 60).

По мнению авторов доклада парламентской ассамблеи НАТО³, проблема терроризма

в Сахеле вытекает из внутренней дестабилизации стран, которая, в свою очередь, является следствием неспособности правительства выполнять все основные функции государства (управление экономикой, предоставление услуг, безопасность). Более того, нехватка ресурсов в результате засухи ведет к внутренним локальным конфликтам, что еще больше усиливает внутреннюю дестабилизацию, которая приводит к появлению терроризма.

Однако, несмотря на то, что проблема терроризма в Сахеле существовала на протяжении нескольких десятилетий, в 2010-х гг. отмечается резкий скачок террористической активности в этом регионе (рис. 1).

На графике видно, что резкий всплеск террористической деятельности произошел в Сахеле после 2010 г., то есть с началом событий «арабской весны». Ключевая характеристика «арабской весны» — коллапс или значительное ослабление авторитарных режимов, которые были довольно эффективны в сдерживании террористической активности. В Сирии, Ливии, Йемене, Ираке и Египте начались затяжные внутренние конфликты. Следует подчеркнуть, что подобное ослабление государств и до «арабской весны» связывалось с усилением террористической активности (Testas, 2004; Vasiliev, 2011; Schumacher & Schraeder, 2021).

Схожую картину можно заметить и на графике рис. 2, где представлено число крупных террористических актов, зафиксированное в странах группы G5 Sahel системой CNTS⁴.

Как было показано М. Шумахером и П. Шредером (Schumacher & Schraeder, 2021), лидеры исламистских террористических

Middle East Special Group (GSM). NATO Parliamentary Assembly. 2020. URL: https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-02/042%20GSM%2020%20E%20rev%202%20fin%20-%20DEVELOPMENT%20AND%20SECURITY%20CHALLENGES%20IN%20THE%20SAHEL%20REGION_0.pdf (accessed: 31.08.2021).

⁴ Cross-National Time-Series Data Archive. Databanks International. URL: <http://www.databanksinternational.com> (accessed: 31.08.2021).

³ Çonkar A. B. Development and Security Challenges in the Sahel Region // Draft Report. Mediterranean and

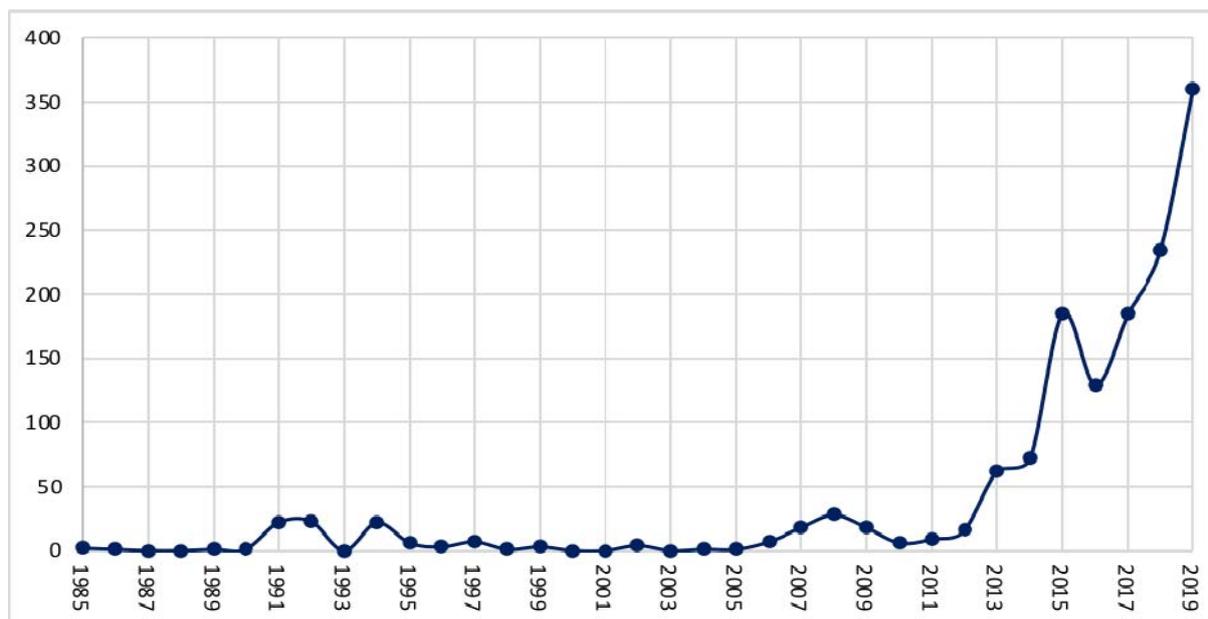


Рис. 1. Динамика террористической активности в странах G5 Sahel в 1985—2019 гг. согласно данным Global Terrorism Database

Источник: составлено авторами. Global Terrorism Database 2021.
URL: <https://www.start.umd.edu/gtd/> (accessed: 29.05.2021).

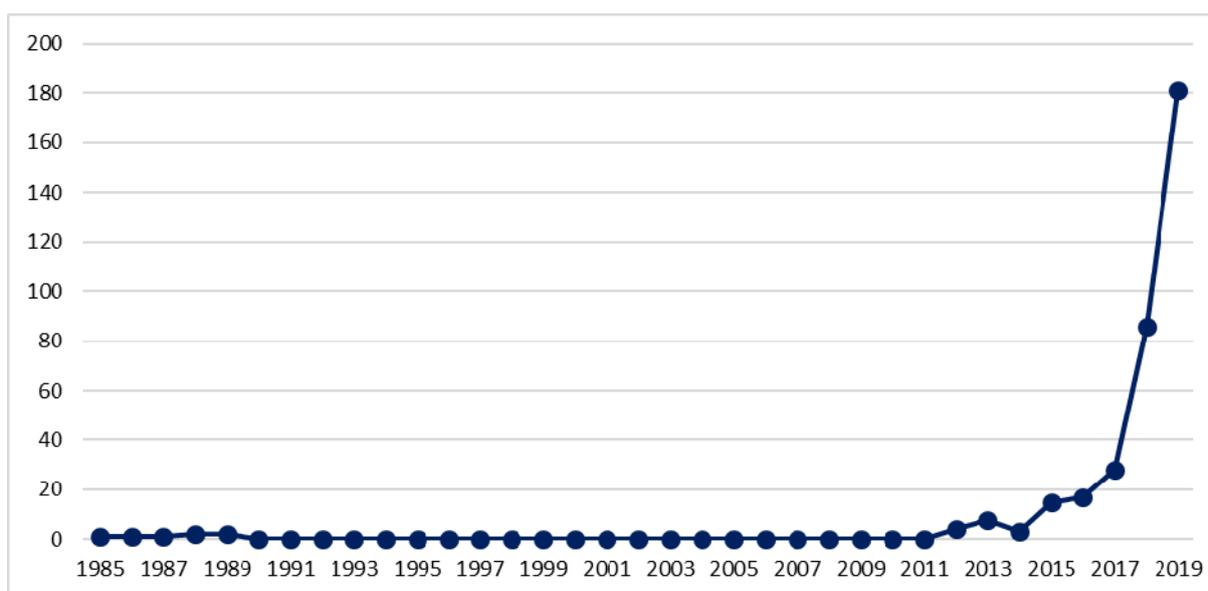


Рис. 2. Динамика террористической активности в странах G5 Sahel в 1985—2019 гг. согласно данным Cross-National Time-Series Data Archive

Источник: составлено авторами. Cross-National Time-Series Data Archive. Databanks International.
URL: <http://www.databanksinternational.com> (accessed: 31.08.2021).

группировок позитивно восприняли революционные события в арабских странах, так как эти события открыли возможность для активизации деятельности исламистов. Падение правящих режимов в Египте и Тунисе, коллапс государственных структур в Ливии и Йемене, а также ослабление центральной

власти в Сирии и Ираке создавали благоприятные условия для появления ИГИЛ (ИГ, ДАИШ, «Исламское государство»)⁵, ячейки которого вскоре стали появляться в разных странах Азии и Африки.

⁵ Организация запрещена в РФ.

Проведенные нами ранее исследования показали, что «арабская весна» сыграла роль триггера начавшейся в 2011 г. волны глобальной социально-политической дестабилизации (Коротаев и др., 2016; Акаев et al., 2017; Grinin et al., 2019; Гринин и др., 2015), которая вылилась в протесты, революции и всплески террористической активности в ряде стран. Такая цепная реакция стала возможной благодаря нескольким механизмам. В первую очередь, следует отметить влияние медиа и социальных сетей на стремительное распространение информации об «арабской весне», ее мотивах и методах. В частности, это привело к росту движения *Оссиру* по всему миру. Однако если

речь идет о ближневосточных странах и соседних регионах, то самое заметное проявление дестабилизации — это волна терроризма. События «арабской весны» привели к возникновению новых террористических группировок (прежде всего ИГИЛ), которым начали присягать на верность террористические организации во всей «афразийской» зоне нестабильности, а также к активизации деятельности старых.

На общем фоне Сахеля динамика террористической активности в Буркина-Фасо имеет свои особенности (рис. 3).

Такая же тенденция фиксируется и базой CNTS (рис. 4).

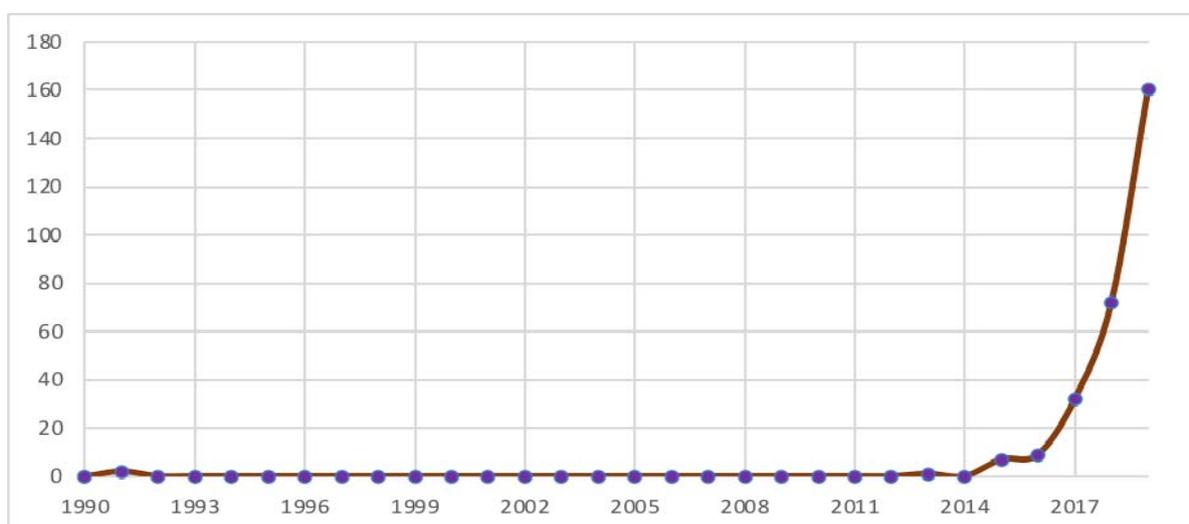


Рис. 3. Динамика террористической активности в Буркина-Фасо в 1990—2019 гг. согласно данным Global Terrorism Database

Источник: составлено авторами. Global Terrorism Database 2021.
URL: <https://www.start.umd.edu/gtd/> (accessed: 29.05.2021).

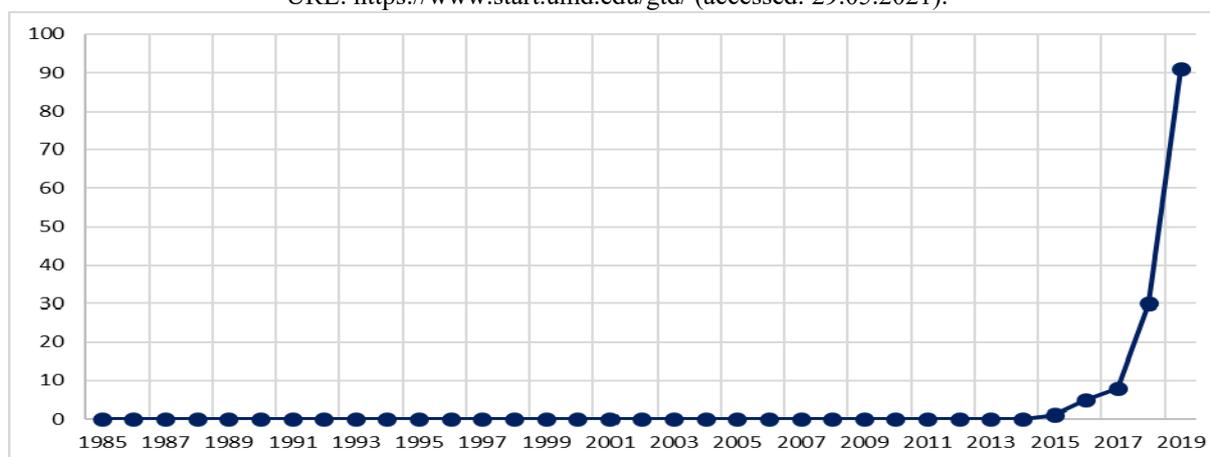


Рис. 4. Динамика террористической активности в Буркина-Фасо в 1985—2019 гг. согласно данным Cross-National Time-Series Data Archive

Источник: составлено авторами. Cross-National Time-Series Data Archive 2021. Databanks International.
URL: <http://www.databanksinternational.com> (accessed: 31.08.2021).

Как мы видим, рост террористической активности в Буркина-Фасо произошел не сразу после «арабской весны», а лишь после 2014 г. При этом особо быстрыми темпами он начал расти после 2015 г. В рамках нашего исследования предпринята попытка осмыслить динамику довольно специфической террористической активности в Буркина-Фасо и ответить на вопрос, почему рост терроризма в Буркина-Фасо наблюдался именно в эти годы.

Динамика террористической активности в Буркина-Фасо

Число терактов в Буркина-Фасо стало расти сразу же после падения режима Б. Компаоре. В Буркина-Фасо, где за весь период 1990—2014 гг. авторитетной международной базой данных Global Terrorism Database было засвидетельствовано всего три теракта, в 2015 г. было зафиксировано уже семь террористических атак⁶. Три основные террористические группы несут ответственность за почти две трети инцидентов насильственного экстремизма в центральноафриканском регионе Сахеля: это Фронт освобождения Масыны (ФЛМ; в 2017 г. вошел в состав альянса Джамат нусрат аль-ислам ва-ль-муслимин (ДНИМ), аффилированного с «Аль-Каидой»⁷), группа Ансар-уль-ислам (также вошедшая в состав ДНИМ) и Исламское государство в Большой Сахаре. Данные группировки сконцентрированы в центральной части Мали, на севере и востоке Буркина-Фасо и на западе Нигера (Hassan, 2020).

Первый после 2013 г. террористический акт произошел в Буркина-Фасо 4 апреля 2015 г., когда на севере страны, недалеко от границы с Мали и Нигером в регионе Липтако-Гурма, был похищен румынский сотрудник службы безопасности⁸. 23 августа 2015 г. в

том же регионе бригада жандармерии подверглась нападению, в результате которого погиб один из бойцов. 9 октября того же года в Саморогуане, на западе Буркина-Фасо, недалеко от малийской границы, три других жандарма были убиты, когда их казармы штурмовали террористы в отместку за арест одного из своих людей⁹.

С 15 января 2016 г., даты первого особо крупного террористического нападения, совершенного в центре Уагадугу на авеню Кваме Нкрума, по 10 декабря 2017 г. Буркина-Фасо стала объектом 102 масштабных нападений воинствующих экстремистов¹⁰. Большинство террористических атак в Буркина-Фасо совершается иностранными организациями, связанными с «Аль-Каидой», обычно из соседнего Мали. Такие организации, как правило, ориентированы на создание «Африканского халифата»¹¹ и подвержены антизападным настроениям. Однако некоторые организации также нацелены на Буркина-Фасо из-за недовольства населения отсутствием экономического развития, что дает подобным группировкам возможность вербовать людей в стране¹².

До 2017 г. большинство атак было совершено «Аль-Каидой в странах исламского Магриба» (АКИМ)¹³, североафриканским отделением «Аль-Каиды», которое базируется в Мали¹⁴. АКИМ проводила атаки по всему

⁹ Ibid.

¹⁰ Sakande M. 105 Attaques Terroristes Contre Le Burkina Faso: Le G5 Sahel, La Solution à Petite Vitesse // Événement. Mars 29, 2018. URL: <https://www.evenement-bf.net/105-attaques-terroristes-contre-le-burkina-faso-le-g5-sahel-la-solution-a-petite-vitesse/> (accessed: 30.07.2021).

¹¹ Bassou A., Guennoun I. Le Sahel Face aux Tendances Al Qaeda et Daech: Quel Dénouement Possible? Al Qaeda vs. Daech in the Sahel: What to Expect? OCP Policy Center, 2017.

¹² Shryock R. Burkina Faso Plagued by Terror Attacks, Rights Allegations // VOA. February 7, 2019. URL: <https://www.voanews.com/a/burkina-faso-plagued-by-terror-attacks-and-human-rights-allegations/4777150.html> (accessed: 30.07.2021).

¹³ Организация запрещена в РФ.

¹⁴ Al-Qaeda Carves Out Its Own Country in Mali // USA Today. December 31, 2012. URL: <https://www.usatoday.com/story/news/world/2012/12/31/al-qaeda-mali/1800787/> (accessed: 30.07.2021).

⁶ Global Terrorism Database. URL: <https://www.start.umd.edu/gtd/> (accessed: 29.05.2021).

⁷ Организация запрещена в РФ.

⁸ Roger B. Attentat de Ouagadougou: pourquoi le Burkina a été frappé? // Jeune Afrique. Janvier 29, 2016. URL: <http://www.jeuneafrique.com/mag/296480/politique/attentat-de-ouagadougou-burkina-a-ete-frappe/> (accessed: 31.08.2021).

Сахелю¹⁵. В частности, АКИМ и ее филиал, группировка «Аль-Мурабитун», взяли на себя ответственность за атаки в Уагадугу в 2016 г.¹⁶ Тогда город подвергся террористическому нападению исламистов. Вооруженные боевики провели 15-часовую осаду отелей и кафе в центре города, в результате чего 28 человек погибли и 56 получили ранения¹⁷.

Другие организации, верные «Аль-Каиде», которые участвуют в террористической деятельности в Буркина-Фасо, включают:

- «Ансар-уль-ислам» («Защитники ислама»), которым руководит радикально настроенный проповедник из Буркина-Фасо. С 2016 по 2018 г. более половины террористических атак в Буркина-Фасо были совершены ею;

- Фронт освобождения Масины, организация из Мали, которая работала с АКИМ;

- Движение за единство и джихад в Западной Африке — отколовшаяся от АКИМ группа.

Вместе с тем в стране действует враждующее с «Аль-Каидой» Исламское государство в Большой Сахаре¹⁸.

Более года Ансар-уль-ислам совместно с «Аль-Каидой в странах исламского Магриба» пыталась распространить терроризм на севере Буркина-Фасо. Это могло пригодиться для создания новых джихадистских союзов, подготовки частей страны к тому, чтобы стать потенциальным убежищем для вербовки и обучения бойцов и транснациональным центром после вероятного поражения

радикальных исламистов в Сирии и Ираке¹⁹. На начальном этапе своего существования Ансар-уль-ислам, основанный М.И. Дико, проповедником из Сум, была проявлением широко распространенного недовольства общественным порядком в этой провинции. Данную организацию можно охарактеризовать как внутреннюю террористическую группировку в Буркина-Фасо, сохраняющую достаточную поддержку, чтобы продолжать восстание низкой интенсивности против местных и национальных властей²⁰.

Джамаат нусрат аль-ислам ва-ль-муслимин (ДНИМ) образовалась в марте 2017 г. в результате слияния АКИМ, «Ансар ад-дин» и «Аль-Мурабитун». ДНИМ остается под контролем АКИМ и базируется в Мали²¹. С момента своего создания ДНИМ осуществила несколько атак в Буркина-Фасо, в том числе взяла на себя ответственность за атаки в Уагадугу (2018 г.)²². ДНИМ представляет особенно серьезную угрозу, поскольку обладает широким набором возможностей, включая высокий уровень летальности терактов, поражение вооруженных целей и координацию нескольких атак одновременно (Zimmerer, 2019).

Также следует отметить, что существует соперничество между «Аль-Каидой» и ИГИЛ, к которому также присоединяются местные группировки. Деятельность ИГИЛ в Буркина-Фасо была ограничена по сравнению

¹⁵ Burkina Faso Arrests Six Over Deadly Militant Attack in January // Reuters. June 2, 2016. URL: <https://www.reuters.com/article/us-burkina-arrests-id-USKCN0YN5WD> (accessed: 30.07.2021).

¹⁶ Guitta O. The Re-emergence of AQIM in Africa // Al-Jazeera. March 20, 2016. URL: <https://www.aljazeera.com/opinions/2016/3/20/the-re-emergence-of-aqim-in-africa/> (accessed: 30.07.2021).

¹⁷ Benedikter R., Ouedraogo I. Extremist Expansion in Burkina Faso: Origins and Solutions // IPI Global Observatory. May 12, 2017. URL: <https://theglobalobservatory.org/2017/05/burkina-faso-extremism-al-qaeda-ansarul-islam/> (accessed: 30.07.2021).

¹⁸ Burkina Faso: Extremism and Terrorism // Counter Extremism Project. URL: <https://www.counterextremism.com/countries/burkina-faso> (accessed: 30.07.2021).

¹⁹ Benedikter R., Ouedraogo I. Extremist Expansion in Burkina Faso: Origins and Solutions // IPI Global Observatory. May 12, 2017. URL: <https://theglobalobservatory.org/2017/05/burkina-faso-extremism-al-qaeda-ansarul-islam/> (accessed: 30.07.2021).

²⁰ The Social Roots of Jihadist Violence in Burkina Faso's North // International Crisis Group. October 12, 2017. URL: <https://www.crisisgroup.org/africa/west-africa/burkina-faso/254-social-roots-jihadist-violence-burkina-fasos-north> (accessed: 30.07.2021).

²¹ Foreign Travel Advice Burkina Faso // GOV.UK. URL: <https://www.gov.uk/foreign-travel-advice/burkina-faso/terrorism> (accessed: 30.07.2021).

²² Jihadist Group Claims Attacks on Military, French Embassy in Burkina Faso // France24. March 3, 2018. URL: <https://www.france24.com/en/20180303-jihadist-group-jsim-claims-burkina-faso-attacks-ouagadougou> (accessed: 30.07.2021).

с деятельностью АКИМ²³. Главный филиал ИГИЛ недалеко от Буркина-Фасо — Исламское государство в Великой Сахаре — был сформирован в мае 2015 г. из отколовшейся фракции «Аль-Мурабитун», присягнувшей ИГИЛ (Warner, 2017). Другой филиал «Исламского государства», Боко Харам, также действует в Буркина-Фасо, но в заметно более ограниченном масштабе (Warner, 2017).

К 2019 г. насилие распространилось с севера страны на восток. В Буркина-Фасо формально никогда не было гражданской войны, но Х. Нсайбия замечает, что нынешний конфликт имеет ее многие ключевые характеристики²⁴.

Эхо ливийского кризиса

То, что теракты в Буркина-Фасо были крайне редки до 2014 г., является в значительной степени заслугой бывшего президента страны Б. Компаоре, деятельность которого была непосредственной причиной удерживания экстремистов вне территории страны. Как показано на рис. 2, в Буркина-Фасо количество террористических атак начало расти сначала после революции 2014 г. и особенно — после неудачного военного переворота 2015 г. Это связано с рядом факторов. Прежде всего, появление терроризма в Буркина-Фасо обусловлено близостью к Мали. Одной из наиболее важных причин распространения терроризма и повстанческих движений в Западной Африке было крушение режима М. Каддафи в Ливии. В начале восстания туарегов исламские группировки, включая «Аль-Каиду в странах исламского Магриба», Движение за единство и джихад в Западной Африке и Ансар ад-дин, сражались вместе с повстанцами²⁵. Ключевую роль здесь сыграли

племена туарегов, которые живут по всему Магрибу и в регионе Сахеля. Во второй половине XX в. многие туареги покинули регион, спасаясь от засухи и политических преследований. Некоторые туареги обосновались в Ливии. Пик притока туарегов пришелся на период с 1970-х по 1990-е гг. (Makariusová & Ludvík, 2012). Начиная с 1970-х гг. в ливийской армии находилось около 12 тыс. туарегов (Danjibo, 2013). Более того, до 1987 г. в Ливии действовало специальное военное подразделение туарегов (называемое «Исламским легионом»), которое создавалось для борьбы с Мали и Чадом (Larémont, 2013). Кроме того, следует также отметить, что многие туареги попали в Ливию в 2011 г. во время ливийской революции в качестве наемников, сражавшихся на стороне М. Каддафи. Когда режим проиграл битву, все эти наемники и солдаты-туареги начали возвращаться обратно в Сахель.

Массовое возвращение вооруженных туарегов, начавшееся в 2011 г., привело к заметному росту политического насилия и террористической активности в Сахеле (Larémont, 2013). Оружие и боеприпасы из Ливии быстро распространились по всему региону. Политическая слабость стран Сахеля и полученное оружие стали предпосылками для новых восстаний туарегов против местных режимов (Danjibo, 2013). Поэтому крах ливийского режима стал важным фактором дестабилизации в регионе. Вместе с влиянием алжирских исламистов массовое возвращение туарегов обусловило появление и развитие радикальных группировок в Сахельском регионе.

Влияние буркинийской революции на рост террористической угрозы в Сахеле

В то же самое время, как уже отмечалось, важную роль в сдерживании террористической угрозы до ноября 2014 г. играл внутренний фактор, связанный с именем президента Б. Компаоре. При нем существовал разведывательный аппарат Буркина-Фасо, который состоял из Координационного центра внутренней

²³ Burkina Faso: Extremism and Terrorism // Counter Extremism Project. URL: <https://www.counterextremism.com/countries/burkina-faso> (accessed: 30.07.2021).

²⁴ Wilkins H. How Has Burkina Faso Changed Since the 'Insurrection'? // Al-Jazeera. November 21, 2020. URL: <https://www.aljazeera.com/news/2020/11/21/how-has-burkina-faso-changed-since-the-insurrection> (accessed: 30.07.2021).

²⁵ Mali: Extremism and Terrorism // Counter Extremism Project. URL: <https://www.counterextremism.com/countries/mali> (accessed: 29.08.2021).

разведки, созданного в 2011 г.²⁶ Центр отвечал за сбор и уточнение информации, передаваемой разведывательными подразделениями в армии, жандармерии и полиции. Руководителем разведывательного аппарата Буркина-Фасо был генерал Ж. Дьендере. Поскольку Ж. Дьендере также отвечал за Президентскую гвардию, она стала главным военным подразделением, связанным с разведывательной сетью Буркина-Фасо²⁷.

Распустив Президентскую гвардию после неудачного военного переворота сентября 2015 г., фактически пытавшегося предоставить Б. Компаоре возможность вернуться к власти, новое руководство лишило страну защиты, которую они имели против джихадистских организаций, готовых проникнуть через границу в Буркина-Фасо. Военнослужащие гвардии были обучены силами Франции и США и даже имели собственное подразделение по борьбе с терроризмом²⁸. Наряду с тем, что Президентская гвардия в Буркина-Фасо была наиболее обученной контртеррористической силой, Б. Компаоре также наладил уникальные отношения с джихадистами в Мали. Фактически Б. Компаоре и его старшие советники, Ж. Дьендере, Д. Бассоле и М. Чафи, в прошлом поддерживали прямые контакты с организациями, связанными с «Аль-Каидой». И М. Чафи, и Ж. Дьендере действовали как посредники между связанными с «Аль-Каидой» группами боевиков и Западом, чтобы обеспечить освобождение западных заложников из плена террористов²⁹.

²⁶ Bamouni D. Fighting Terrorism in Burkina Faso // Defense WEB. February 15, 2017. URL: <https://www.defencweb.co.za/joint/diplomacy-a-peace/fighting-terrorism-in-burkina-faso/> (accessed: 29.08.2021).

²⁷ Ben-Zur B., Toole G. Burkina Faso Security: Threats, Challenges, Response // IDC Herzliya. March 24, 2020. URL: https://www.ict.org.il/Article/2521/Burkina_Faso_Security#gsc.tab=0 (accessed: 29.08.2021).

²⁸ Penney J. Blowback in Africa: How America's Counterterrorism Strategy Helped Destabilize Burkina Faso // The Intercept. November 22, 2018. URL: <https://theintercept.com/2018/11/22/burkina-faso-us-relations/> (accessed: 29.08.2021).

²⁹ Ben-Zur B., Toole G. Burkina Faso Security: Threats, Challenges, Response // IDC Herzliya. March 24, 2020. URL: https://www.ict.org.il/Article/2521/Burkina_Faso_Security#gsc.tab=0 (accessed: 29.08.2021).

В 2009 г. личный советник Б. Компаоре М. Чафи провел переговоры с АКИМ об освобождении канадских заложников³⁰.

Аналогичным образом в 2012 г. Ж. Дьендере координировал освобождение итальянских и испанских заложников³¹. Сам Б. Компаоре выступил посредником между Экономическим сообществом стран Западной Африки (ЭКОВАС) и Ансар ад-дин во время кризиса в Мали в 2012 г. Б. Компаоре дважды принимал членов Ансар ад-дин в Уагадугу для переговоров³². Вдобавок Д. Бассоле однажды побывал в Мали в 2012 г., где и встретился с И. Аг Гали, основателем Ансар ад-дин³³. Отставка Б. Компаоре разрушила все неформальные связи и договоренности, которые режим налаживал с региональными джихадистскими организациями, развязав им руки для достаточно быстрого и легкого проникновения в Буркина-Фасо³⁴.

Заключение

Буркина-Фасо представляет собой достаточно своеобразный случай дестабилизации в Сахеле. Рост террористической активности в стране носит отличный от других сахельских кейсов характер, так как страна, по сути, пережила свою собственную «арабскую весну» с задержкой в несколько лет от основной волны.

Долгое время в Буркина-Фасо практически не наблюдалось террористической актив-

³⁰ Thurston A. Escalating Conflicts in Burkina Faso // RLS Research Papers on Peace and Conflict Studies in West and Central Africa. June 30, 2021. URL: <https://rosalux.sn/en/escalating-conflicts-burkina-faso-alex-thurston/> (accessed: 29.08.2021).

³¹ Bonkougou M. Freed Italian, Spanish Hostages Head for Europe // Reuters. July 19, 2012. URL: <https://www.reuters.com/article/us-mali-hostages-idUSBRE86I0JQ20120719> (accessed: 29.08.2021).

³² Thurston A. Escalating Conflicts in Burkina Faso // RLS Research Papers on Peace and Conflict Studies in West and Central Africa. June 30, 2021. URL: <https://rosalux.sn/en/escalating-conflicts-burkina-faso-alex-thurston/> (accessed: 29.08.2021).

³³ Ibid.

³⁴ Ben-Zur B., Toole G. Burkina Faso Security: Threats, Challenges, Response // IDC Herzliya. March 24, 2020. URL: https://www.ict.org.il/Article/2521/Burkina_Faso_Security#gsc.tab=0 (accessed: 29.08.2021).

ности. Во многом этому способствовали относительная этническая однородность (большинство населения составляет народ моси) и, как следствие, отсутствие острых межэтнических конфликтов. Можно отметить отсутствие в Буркина-Фасо значительных всплесков террористической активности вплоть до 2015 г.

В 2014 г. в Буркина-Фасо начались протесты против власти президента Б. Компаоре, который к этому моменту правил на протяжении 27 лет³⁵. Триггером для протестов стали попытки внести в конституцию страны поправки, которые должны были увеличить президентский срок. Данные протесты завершились в конце октября 2014 г. революционным свержением режима президента Компаоре.

³⁵ Patinkin J. Could Burkina Faso Protests Signal End of President's 27-year Rule // The Christian Science Monitor. October 30, 2014. URL: <https://www.csmonitor.com/World/Africa/2014/1030/Could-Burkina-Faso-protests-signal-end-of-president-s-27-year-rule> (accessed: 29.08.2021).

Попытка военного переворота в сентябре 2015 г. усилила дестабилизацию в стране³⁶.

В 2014—2015 гг. в Буркина-Фасо, по сути, включились те же самые механизмы социально-политической дестабилизации, что и в странах «арабской весны» в 2011 г. В результате падения авторитарного режима Б. Компаоре Буркина-Фасо столкнулась с аналогичными для Египта, Йемена и других стран «арабской весны» проблемами, в том числе неспособностью постреволюционных властей эффективно бороться с терроризмом.

Таким образом, несмотря на несколько разных сценариев распространения терроризма по региону, следует отметить, что во всех случаях стартовым триггером послужили именно события «арабской весны».

³⁶ Лидеры государственного переворота закрыли границы Буркина-Фасо // ТАСС. 17.09.2015. URL: <https://tass.ru/mezhdunarodnaya-panorama/2269825> (дата обращения: 29.08.2021).

Поступила в редакцию / Received: 21.11.2021
Доработана после рецензирования / Revised: 14.04.2022
Принята к публикации / Accepted: 18.04.2022

Библиографический список

- Гринин Л. Е., Исаев Л. М., Коротаев А. В. Революции и нестабильность на Ближнем Востоке. Москва : Учитель, 2015.
- Исаев Л. М., Айсин М., Медведев И. А., Коротаев А. В. Исламский терроризм на Ближнем Востоке и его влияние на мировую безопасность // Вестник Российского университета дружбы народов. Серия: Политология. 2020. Т. 22, № 4. С. 713—730. <https://doi.org/10.22363/2313-1438-2020-22-4-713-730>
- Коротаев А. В., Исаев Л. М., Руденко М. А. Формирование африканской зоны нестабильности // Восток. Афро-Азиатские общества: история и современность. 2015. № 2. С. 88—99.
- Коротаев А. В., Медведев И. А., Мещерина К. В. Связь религиозных ценностей с уровнем террористической активности: предварительные результаты количественного анализа // Системный мониторинг глобальных и региональных рисков : Ежегодник. Вып. 10 / отв. ред. Л. Е. Гринин, А. В. Коротаев, К. В. Мещерина. Волгоград : Издательство «Учитель», 2019. С. 400—423.
- Коротаев А. В., Шишкина А. Р., Исаев Л. М. Арабская весна как триггер глобального фазового перехода? // Полис. Политические исследования. 2016. № 3. С. 108—122. <https://doi.org/10.17976/jpps/2016.03.09>
- Akaev A. A., Korotayev A. V., Issaev L. M., Zinkina J. V. Technological Development and Protest Waves: Arab Spring as a Trigger of the Global Phase Transition? // Technological Forecasting and Social Change. 2017. Vol. 116. P. 316—321. <https://doi.org/10.1016/j.techfore.2016.08.009>
- Attiya I. Li-tahdid al-munazamat wa al-irhab: masadir jadida li-tahdid al-amn fi Ifriqiya // Macallatul-buhus wad-dirasatil-qanuniyya was-siyasiyya [Organized Crime and Terrorism: New Sources of Security Threats in Africa // Journal of Legal and Political Research]. 2017. No. 8. P. 53—70. (На арабском языке).
- Danjibo N. D. The Aftermath of the Arab Spring and Its Implication for Peace and Development in the Sahel and Sub-Saharan Africa // The Strategic Review for Southern Africa. 2013. Vol. 35, no. 2. P. 16—34. <https://doi.org/10.35293/srsa.v35i2.135>
- Dentice G. Terrorism in the Sahel Region: An Evolving Threat on Europe's Doorstep // Euromesco: Policy Brief. 2018. No. 80. P. 1—14.

- Grinin L. E., Korotayev A. V., Tausch A.* Islamism, Arab Spring and Democracy: World System and World Values Perspectives. Cham : Springer, 2019. <https://doi.org/10.1007/978-3-319-91077-2>
- Hassan H.* A New Hotbed for Extremism? Jihadism and Collective Insecurity in the Sahel // *Asian Journal of Peacebuilding*. 2020. Vol. 8, no. 2. P. 203—222. <https://doi.org/10.18588/202011.00a120>
- Issaev L. M., Fain E., Korotayev A. V.* Impact of the Arab Spring on Terrorist Activity in the Sahel // *Ideology and Politics Journal*. 2021. Vol. 19, no. 3. P. 34—49. <https://doi.org/10.36169/2227-6068.2021.03.00003>
- Larémont R. R.* After the Fall of Qaddafi: Political, Economic, and Security Consequences for Libya, Mali, Niger, and Algeria // *Stability: International Journal of Security and Development*. 2013. Vol. 2, no. 2. P. 1—8. <http://doi.org/10.5334/sta.bq>
- Makariusová R., Ludvík Z.* Non-state Military Actors: The Case of the 2011 Libyan Conflict // *Central European Journal of International & Security Studies*. 2012. Vol. 6. P. 244—268.
- Nyadera I., Massaoud H.* Elusive Peace and the Impact of Ungoverned Space in the Sahel Conflict // *Güvenlik Bilimleri Dergisi*. 2019. Vol. 8, no. 2. P. 271—288. <https://doi.org/10.28956/gbd.646327>
- Schumacher M. J., Schraeder P. J.* Does Domestic Political Instability Foster Terrorism? Global Evidence from the Arab Spring Era (2011—14) // *Studies in Conflict & Terrorism*. 2021. Vol. 44, no. 3. P. 198—222. <https://doi.org/10.1080/1057610X.2018.1538124>
- Testas A.* Determinants of Terrorism in the Muslim World: An Empirical Cross-Sectional Analysis // *Terrorism and Political Violence*. 2004. Vol. 16, no. 2. P. 253—273. <https://doi.org/10.1080/09546550490482504>
- Vasiliev A. M.* The Tsunami of Revolutions: New Geopolitical Realities // *Insight on Africa*. 2011. Vol. 3, no. 2. P. 117—128. <https://doi.org/10.1177%2F0975087814411137>
- Warner J.* Sub-Saharan Africa's Three 'New' Islamic State Affiliates // *CTC Sentinel*. 2017. Vol. 10, no. 1. P. 28—32.
- Zimmerer M.* Terror in West Africa: A Threat Assessment of the New Al Qaeda Affiliate in Mali // *Critical Studies on Terrorism*. 2019. Vol. 12, no. 3. P. 491—511. <https://doi.org/10.1080/17539153.2019.1599531>

Сведения об авторах: *Исаев Леонид Маркович* — кандидат политических наук, доцент, заместитель заведующего научно-учебной лабораторией мониторинга рисков социально-политической дестабилизации факультета социальных наук НИУ ВШЭ, старший научный сотрудник Центра цивилизационных и региональных исследований Института Африки РАН, старший научный сотрудник кафедры африканистики и арабистики Российского университета дружбы народов; ORCID: 0000-0003-4748-1078; e-mail: lisaev@hse.ru

Коротаев Андрей Витальевич — доктор исторических наук, профессор, заведующий научно-учебной лабораторией мониторинга рисков социально-политической дестабилизации факультета социальных наук НИУ ВШЭ, ведущий научный сотрудник Центра цивилизационных и региональных исследований Института Африки РАН, ведущий научный сотрудник кафедры африканистики и арабистики Российского университета дружбы народов; ORCID: 0000-0003-3014-2037; e-mail: akorotaev@hse.ru

Бобарыкина Дарья Алексеевна — магистрант Санкт-Петербургской школы социальных наук и востоковедения НИУ ВШЭ в Санкт-Петербурге; ORCID: 0000-0002-7722-1931; e-mail: d.bobarykina@mail.ru



РЕЦЕНЗИИ

BOOK REVIEWS

DOI: 10.22363/2313-0660-2022-22-2-422-424

Рецензия на книгу :
**Buchanan B. The Hacker and the State:
Cyber Attacks and the New Normal of Geopolitics.**
Cambridge, Massachusetts : Harvard University Press, 2020. 309 p.

И.О. Яникеева  

МГИМО МИД России, Москва, Российская Федерация

 yanikeeva93@mail.ru

Для цитирования: Яникеева И. О. Рецензия на книгу : Buchanan B. The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Cambridge, Massachusetts : Harvard University Press, 2020. 309 p. // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 422—424. <https://doi.org/10.22363/2313-0660-2022-22-2-422-424>

Book review:
**Buchanan, B. (2020). The Hacker and the State:
Cyber Attacks and the New Normal of Geopolitics.**
Cambridge, Massachusetts: Harvard University Press, 309 p.

Inna O. Yanikeeva  

MGIMO University, Moscow, Russian Federation

 yanikeeva93@mail.ru

For citation: Yanikeeva, I. O. (2022). Book review: Buchanan, B. (2020). The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Cambridge, Massachusetts: Harvard University Press, 309 p. *Vestnik RUDN. International Relations*, 22(2), 422—424. (In Russian). <https://doi.org/10.22363/2313-0660-2022-22-2-422-424>

В XXI в. эксперты уделяют значительное внимание анализу влияния новых акторов на геополитику в условиях цифровизации, что, в свою очередь, воздействует на обеспечение международной информационной безопасности (МИБ). Одним из примеров работ по

данной тематике является монография «Хакер и государство: кибератаки и новая норма геополитики» Б. Бьюкенена¹, специалиста в области кибербезопасности, ведущего сотрудника Центра безопасности и новейших технологий в Школе дипломатической службы при

¹ Б. Бьюкенен проводит исследования на стыке кибербезопасности и искусства управления государством.

© Яникеева И.О., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

Джорджтаунском университете, автора книги «Дилемма кибербезопасности», опубликованной в 2017 г.

Рецензируемая монография посвящена актуальной проблеме влияния хакеров на геополитику. Научная значимость данного труда возрастает в свете событий, происходящих в XXI в.: несанкционированное вредоносное вмешательство в работу какой-либо информационной системы, кражи информации через компьютерные сети, распространение вредоносных программ, кражи номеров банковских карт и банковских реквизитов. Все указанные процессы подчеркивают востребованность широких комплексных исследований, связанных с цифровой средой в целом и научную ценность данной монографии в частности.

Многие эксперты ожидали, что кибервойна будет цифровой версией взаимного гарантированного уничтожения в ходе ядерной войны. Однако время продемонстрировало, что кибератаки наиболее эффективны в условиях скрытности и отрицания собственных действий в ходе непрерывного столкновения в цифровой среде. Кибератаки стали неотъемлемой частью геополитической конкуренции. По словам Б. Бьюкенена, правительственные хакеры ведут бесконечную игру шпионажа и обмана, атак и контратак, дестабилизации и возмездия (Buchanan, 2020).

Как хакеры влияют на геополитику? Автор отвечает на свой исследовательский вопрос, опираясь на более чем десятилетние наблюдения, эмпирические данные и инвентаризацию.

По его словам, на сегодняшний день одним из основных способов, которыми правительства формируют геополитику, является осуществление кибервзломов других стран. Посредством хакеров государства способны прослушивать, шпионить, изменять и воровать данные, саботировать работу систем, разрушать инфраструктуру, атаковать, манипулировать, разоблачать и дестабилизировать государства-цели.

Монография хорошо фундирована, опирается на обширный круг источников и литературы, которые позволяют автору комплексно исследовать проблематику осуществления кибератак в геополитических целях. В

качестве метатеории исследования автор использует политический реализм, исследуя кибератаки в качестве преступлений, совершенных не отдельными группировками или хакерами, а государствами, которые за ними стоят.

Сильной стороной исследования является структура изложения, акцент не только на самих фактах кибератак, но и на анализе информации: кто, как и почему это осуществлял. Это позволило автору обосновать вывод, что хакеры, работающие на государства, против них и внутри них, формируют мир.

Б. Бьюкенен использовал системный подход для анализа международных отношений в условиях непрерывного ведения киберпротивоборства, что позволило ему классифицировать кибероперации и выявить их закономерности, а именно показать, что они оказываются малоэффективными в изменении политического курса государств, но весьма действенными в качестве инструмента политического давления и донесения до оппонентов своей позиции по различным пунктам международной повестки.

В книге освещена деятельность всех ключевых акторов, имеющих стратегические интересы в цифровой среде, — США, Ирана, Китая, КНДР и России. Вместе с тем роль России изучена в недостаточной степени. Информация о киберпреступниках, якобы связанных с российским правительством, опирается в большей степени на домыслы и предположения, а не на выявленные факты, как это было в случае с США, когда доказательства их кибердеятельности были опубликованы в открытом доступе (речь идет, в частности, о Shadow Brokers) и не было сомнений в их причастности к кибератакам. Кроме того, учитывая, что Б. Бьюкенен согласовывал текст книги с представителями спецслужб США, о чем он пишет в разделе «Благодарности», говорить о беспристрастности в опубликовании информации о России не представляется возможным.

Работа Б. Бьюкенена состоит из трех частей, каждая из которых включает несколько глав, посвященных явлениям кибершпионажа, кибернападений и дестабилизации посредством кибератак. Книга показывает, что государства совершают все

более решительные взломы в процессе борьбы за превосходство на мировой арене. В каждой из 13 глав исследуется отдельная цель кибервзломов и приводятся примеры, их демонстрирующие.

На протяжении всей книги Б. Бьюкенен отмечает три основные характеристики хакерской деятельности: 1) ее универсальность как инструмента геополитического влияния, 2) слабость — как средства геополитического сигнализирования и 3) амбициозность, принимающая все более агрессивный характер по мере того, как современные кибероперации наращивают свои возможности.

Среди основных выводов автора необходимо отметить следующие:

— государства время от времени осуществляют кибероперации для получения преимуществ перед другими государствами путем кибершпионажа, нападений и дестабилизации;

— кибервозможности не вечны;

— хакеры во многих случаях находятся вне досягаемости целей кибератак, в связи с чем обвинительные заключения являются не более чем подробными пресс-релизами, но недостаточными для управления государством;

— риторика вокруг таких тем, как киберсдерживание, иногда может опережать реальность, заключающуюся в том, что кибервозможности редко предлагают четкие и достоверные средства сигнализирования и принуждения. Государства иногда пытаются сигнализировать с помощью киберопераций, но обычно терпят неудачу; даже в идеальных условиях сигнализирование посредством киберопераций может быть недостаточным;

— хакеры играют значимую роль в системе управления государством. Самый изолированный и находящийся под санкциями режим в мире (КНДР) частично финансирует себя за счет хакерских атак, что служит примером пересечения государственного управления и киберопераций;

— кибератаки могут быть использованы совместно с обычными вооружениями.

Книга демонстрирует, как хакеры меняют геополитику, выполняя все более разнообразные миссии, развивая все более мощные возможности для получения геополитического преимущества для своих государств, и их действия не сдерживаются нормами, соглашениями или страхом возмездия. По мнению автора, в условиях конфликта интересов, желаний и мировоззрений государства продолжают взламывать друг друга. Их хакеры, не сдерживаемые ничем, будут продолжать менять мир, влияя на геополитику. Кибероперации продолжают становиться более мощными и масштабными.

Монография обладает потенциалом, связанным с дальнейшей научной разработкой и детализацией тех проблем, которые в ней обозначены. К числу таких проблем относится анализ роли России в глобальной цифровой среде и связанный с этим потенциал политической конфликтности, а также подробный анализ роли хакеров в процессе обеспечения МИБ. Работа представляет интерес как для исследователей-международников, так и для практиков в сфере государственного управления, занимающихся планированием и реализацией проектов, связанных с обеспечением МИБ.

Поступила в редакцию / Received: 18.12.2021

Принята к публикации / Accepted: 18.04.2022

Библиографический список / References

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Cambridge, Massachusetts: Harvard University Press.

Сведения об авторе: Яникеева Инна Олеговна — аспирант кафедры мировых политических процессов Московского государственного института международных отношений МИД Российской Федерации; ORCID: 0000-0001-9590-5301; e-mail: yanikeeva93@mail.ru

About the author: Yanikeeva Inna Olegovna — PhD Student, Department of World Political Processes, Moscow State Institute of International Relations (MGIMO University); ORCID: 0000-0001-9590-5301; e-mail: yanikeeva93@mail.ru



DOI: 10.22363/2313-0660-2022-22-2-425-428

Рецензия на книгу :
**Kharas H., McArthur J. W., Ohno I. Breakthrough:
The Promise of Frontier Technologies for Sustainable Development.
Brookings Institution Press, 2022. 256 p.**

Л.А. Мелконян✉

Российский университет дружбы народов, Москва, Российская Федерация

✉melkonyan-la@rudn.ru

Для цитирования: Мелконян Л. А. Рецензия на книгу : Kharas H., McArthur J. W., Ohno I. Breakthrough: The Promise of Frontier Technologies for Sustainable Development. Brookings Institution Press, 2022. 256 p. // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 425—428. <https://doi.org/10.22363/2313-0660-2022-22-2-425-428>

Book review:
**Kharas, H., McArthur, J. W., & Ohno, I. (2022). Breakthrough:
The Promise of Frontier Technologies for Sustainable Development.
Brookings Institution Press, 256 p.**

Lusine A. Melkonyan✉

Peoples' Friendship University of Russia, Moscow, Russian Federation

✉melkonyan-la@rudn.ru

For citation: Melkonyan, L. A. (2022). Book review: Kharas, H., McArthur, J. W., & Ohno, I. (2022). Breakthrough: The Promise of Frontier Technologies for Sustainable Development. Brookings Institution Press, 256 p. *Vestnik RUDN. International Relations*, 22(2), 425—428. (In Russian). <https://doi.org/10.22363/2313-0660-2022-22-2-425-428>

Пандемия COVID-19 преподала современному миру множество уроков, среди которых одним из важнейших является роль технологий в решении на первый взгляд неразрешимых проблем. Прорывные технологии в кратчайшие сроки привели к разработке вакцин против COVID-19, тем самым способствуя замедлению роста пандемии, приведшей к смерти по меньшей мере 5 млн человек и

вызавшей необратимые социально-экономические и политические процессы по всему миру.

В этой связи научный исследовательский интерес вызывает работа экспертов и исследователей Брукингского института (Brookings Institution)¹ и Исследовательского института мира и развития Огата при Японском агентстве международного сотрудничества (JICA Ogata

¹ About Brookings Institution // The Brookings Institution. URL: <https://www.brookings.edu/about-us/> (accessed: 10.04.2022).

© Мелконян Л.А., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

Research Institute for Peace and Development)² под редакцией Хоми Хараса, Джона В. Макарттура и Изуми Оно *Breakthrough: The Promise of Frontier Technologies for Sustainable Development* (Kharas, McArthur & Ohno, 2022). Название работы можно перевести на русский язык как «Прорыв: перспектива передовых технологий для устойчивого развития» или «Перспективы применения прорывных технологий в целях устойчивого развития».

Прежде чем перейти к обзору данной монографии, увидевшей свет 25 января 2022 г., следует сказать несколько слов о ее авторах. Хоми Харас (Homi Kharas) — старший научный сотрудник Центра устойчивого развития при Брукингском институте. Х. Харас является специалистом в области глобального управления, помощи бедным и развивающимся странам. Он является автором целого ряда публикаций о глобальной политике развития, глобальных тенденциях, продовольственном кризисе, международных организациях, G20, Комитете содействия развитию и частной благотворительности.

Джон В. Макарттур — старший научный сотрудник и директор Центра устойчивого развития Брукингского института. Он также является старшим советником Фонда ООН и членом Совета управляющих Международного исследовательского центра развития. Макарттур преподавал в Школе международных и общественных отношений Колумбийского университета (Columbia SIPA), а также возглавлял советы по глобальной повестке дня Всемирного экономического форума и был членом Консультативного совета форума по вопросам устойчивого развития и конкурентоспособности. Среди последних работ Х. Хараса и Дж.В. Макарттура следует выделить *Leave No One Behind: Time for Specifics on the Sustainable Development Goals* (Kharas, McArthur & Ohno, 2019), *From Summits to Solutions: Innovations in Implementing the*

Sustainable Development Goals (Kharas, McArthur, Desai & Kato, 2018) и др.

Изуми Оно — старший научный консультант исследовательского института JICA Ogata, профессор Национального института политических исследований (GRIPS)³. И. Оно является специалистом в области политики международного развития, сотрудничества в целях развития и бизнеса. Среди последних публикаций автора следует отметить *Industrial Human Resource Development in Developing Countries: Knowledge and Skills in the Era of SDGs* (Ohno, 2021), *Leave No One Behind: Time for Specifics on the Sustainable Development Goals* (Kharas, McArthur & Ohno, 2019) и др.

Центральный вопрос, лежащий в основе рецензируемой монографии, — каковы вероятные технологические достижения, которые могут способствовать достижению Целей ООН в области устойчивого развития (ЦУР). Авторы исследования отмечают, что заглядывать в будущее сложно и проблематично, однако для ученых полезно представлять, какие инновации могут решить сегодняшние проблемы и сделать завтрашний день лучше.

Книга состоит из 12 глав, в которых 18 выдающихся международных экспертов исследуют потенциал и перспективы технологических прорывов, описывая свое видение того, каким образом технологии будущего могут повлиять на условия жизни человечества и окружающую среду в течение следующего десятилетия. Отражены представления авторов о будущих успехах человечества с помощью прорывных технологий в различных областях.

В первой главе «Прорывы: зачем они нужны для устойчивого развития» Х. Харас, Дж.В. Макарттур и И. Оно отмечают, что процесс технологических изменений будет достаточно сложным и в будущем. Новые прорывные технологии с социальной точки зрения должны расширять возможности

² Our Vision and Basic Policy // JICA Ogata Research Institute for Peace and Development. URL: <https://www.jica.go.jp/jica-ri/about/policy.html> (accessed: 08.04.2022).

³ About GRIPS // National Graduate Institute for Policy Studies (GRIPS). URL: <https://www.grips.ac.jp/en/about/index-6/> (accessed: 10.04.2022).

людей, сокращать неравенство и защищать конфиденциальность, одновременно укрепляя доверие к правительствам, науке и другим институтам. Необходимо также смириться с тем фактом, что технологии не решат все проблемы и сразу: технологии должны развиваться и адаптироваться к новым условиям и обществу пользователей, а развитие технологий должно сопровождаться трезвыми дебатами о том, зачем нужны эти технологии, как они работают и кто в конечном итоге от них выиграет. Конкретных ответов на эти вопросы у авторов нет, поскольку ответы в будущем будут сильно зависеть от контекстов (*context-specific*). Каждое достижение в развитии науки, разработке прорывных технологий и создании новых систем потребует человеческой изобретательности, ресурсов и настойчивости. Гарантий прогресса нет, но формирование представлений о такой возможности — первый шаг к достижению мира устойчивого развития для всех.

Авторы второй главы «Прорывные технологии для обеспечения готовности к пандемии» И. Ботти-Лодовико и П. Сабети утверждают, что мир не может противостоять вызовам и проблемам устойчивого развития, не разработав план по выявлению и сдерживанию инфекционных заболеваний. Ни одна страна, регион или сфера деятельности не могут противостоять в одиночку, когда речь идет о борьбе с пандемией. Такие проблемы, как неравенство, несправедливость, бедность и отсутствие продовольственной безопасности во время вспышки пандемии, не только выходят на первый план, но и усугубляются из-за нагрузки на национальную инфраструктуру. COVID-19 служит доказательством и еще одним напоминанием об этой действительности, призывая страны инвестировать в справедливую и эффективную инфраструктуру здравоохранения и расширять возможности сообществ, чтобы они реально участвовали в обеспечении готовности к пандемии и реагировании на нее. Авторы в качестве

качественного и справедливого решения проблем системы здравоохранения видят применение комплексных подходов с использованием прорывных, передовых технологий.

Третья и последующие главы данной книги также охватывают широкий спектр проблем и затрагивают вопросы прорывных технологических решений в таких областях, как медицина, сельское хозяйство, энергетика, финансы и охрана окружающей среды.

Рецензируемая монография отражает основные перспективы развития человечества, однако выводы авторов следует рассматривать не в качестве прогнозов, а как обоснованные предположения и представления исследователей о том, что может произойти, если лидеры стран сделают правильный выбор и создадут необходимые обстоятельства для технологического прорыва.

Подводя итог, следует отметить, что для достижения поставленных целей устойчивого развития к 2030 г. потребуются прорывы в науке, разработке новых продуктов, товаров и услуг, а также в институциональных системах.

Технический прогресс не решит всех мировых проблем. Для преодоления новых вызовов необходима государственная политика, более ориентированная на общество и решение проблем социума. Однако в этом деле решающую роль должны и будут играть технологии, в том числе направленные на достижение лучших результатов в области устойчивого развития.

Монография Х. Хараса, Дж.В. Макартура и И. Оно является важным напоминанием о том, что перспектива лучшего будущего в целом ряде областей находится в пределах нашей досягаемости. Монография предназначена для специалистов и исследователей в области политики ООН, передовых технологий, международной безопасности, устойчивого развития, а также для широкого круга читателей, интересующихся экономическим, социальным и экологическим будущим мира.

Поступила в редакцию / Received: 11.04.2022
Принята к публикации / Accepted: 18.04.2022

Библиографический список / References

- Kharas, H., McArthur, J., & Ohno, I. (2019). *Leave no one behind: Time for specifics on the Sustainable Development Goals*. Brookings Institution Press.
- Kharas, H., McArthur, J., & Ohno, I. (2022). *Breakthrough: The promise of frontier technologies for sustainable development*. Brookings Institution Press.
- Kharas, H., McArthur, J., Desai, R., & Kato, H. (2018). *From summits to solutions: Innovations in implementing the Sustainable Development Goals*. Brookings Institution Press.
- Ohno, I. (2021). *Industrial human resource development in developing countries: Knowledge and skills in the era of SDGs*. Nippon Hyoronsha.

Сведения об авторе: Мелконян Лусине Арменовна — ассистент кафедры теории и истории международных отношений Российского университета дружбы народов; e-mail: melkonyan-la@rudn.ru

About the author: Melkonyan Lusine Armenovna — Assistant, Department of Theory and History of International Relations, Peoples' Friendship University of Russia (RUDN University); e-mail: melkonyan-la@rudn.ru

DOI: 10.22363/2313-0660-2022-22-2-429-432

Рецензия на книгу :
Simon H. Hidden Champions: The New Game in the Chinese Century.
Frankfurt — New York : Campus, 2021. 280 p.

Е.Л. Андреева  , А.В. Ратнер 

Институт экономики Уральского отделения РАН, Екатеринбург, Российская Федерация
andreeva.el@uiec.ru

Для цитирования: Андреева Е. Л., Ратнер А. В. Рецензия на книгу : Simon H. Hidden Champions: The New Game in the Chinese Century. Frankfurt — New York : Campus, 2021. 280 p. // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 429—432. <https://doi.org/10.22363/2313-0660-2022-22-2-429-432>

Book review:
Simon, H. (2021). Hidden Champions: The New Game in the Chinese Century.
Frankfurt — New York: Campus, 280 p.

Elena L. Andreeva  , Artem V. Ratner 

Institute of Economics of the Ural Branch of RAS, Yekaterinburg, Russian Federation
andreeva.el@uiec.ru

For citation: Andreeva, E. L., & Ratner, A. V. (2022). Book review: Simon, H. (2021). Hidden champions: The new game in the Chinese century. Frankfurt — New York: Campus, 280 p. *Vestnik RUDN. International Relations*, 22(2), 429—432. (In Russian). <https://doi.org/10.22363/2313-0660-2022-22-2-429-432>

В контексте обсуждения технологических возможностей «Глобального Юга» и осуществления им технологического трансфера может быть отмечена новая книга немецкого почетного доктора, профессора, единственного от Германии входящего в список *Thinkers 50 Hall of Fame*, включающего наиболее влиятельных в мире мыслителей в области менеджмента, председателя международной консалтинговой фирмы Simon-Kucher & Partners, автора концепции «скрытых чемпионов» Г. Саймона *Hidden Champions: The New Game in the Chinese Century* (нем. *Hidden Champions: die neuen Spielregeln in den chinesischen Jahrhundert*).

Одна из гипотез, выдвигаемых и доказываемых в книге, — о будущем существенном влиянии Китая на условия функционирования международной экономики, в том числе посредством компаний — «скрытых чемпионов», феномена, который вот уже 30 лет исследуется профессором Г. Саймоном. Все началось в 1987 г. с вопроса гарвардского профессора Т. Левитта на встрече в Дюссельдорфе: «Почему немецкие компании так успешны в экспорте?» Годом ранее Германия впервые стала лидером мирового экспорта. Т. Левитта интересовали источники конкурентных преимуществ стран и компаний, и он популяризовал термин «глобализация» благодаря

© Андреева Е.Л., Ратнер А.В., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

высокорейтинговой статье в *Harvard Business Review* (Levitt, 1983). Поиск ответа на вопрос Т. Левитта привел к многолетним исследованиям и появлению еще одного популярного термина — «скрытые чемпионы» (СЧ). Система Google находит 1,75 млн страниц на запрос этого словосочетания. За это время Г. Саймон опубликовал более 35 книг на 27 языках, включая бестселлер *Hidden Champions — Lessons from 500 of the World's Best Unknown Companies* (Simon, 1996) и его перевод на русский язык (Саймон, 2005), выполненный Е.Л. Андреевой. Первый соавтор данной рецензии тоже познакомилась с книгой Г. Саймона в ходе работы над докторской диссертацией, защищенной как раз в 2005 г., и проведения анкетирования в отношении процессов глобализации. Сегодня их развитие претерпевает глубочайшие изменения. Поиск ответа на вопрос, что же мы переживаем сегодня: «похоронный марш глобализации», этап деглобализации или новый цифровой формат глобализации, — также послужит возможностью продолжить дальнейшие исследования.

В своей новой книге Г. Саймон актуализирует концепцию «скрытых чемпионов» с учетом современных трендов развития глобальной экономики, один из которых — активизация развивающихся стран, в первую очередь Китая. Это фигурирует и в названии монографии, определившем за Китаем характеристику переживаемой эпохи. Необходимо также отметить некоторое отличие названий англо- и немецкоязычного изданий. Если в английской версии речь идет о «новой игре» (*New Game*), то в немецкой — о новых «правилах игры» (*neue Spielregeln*). Эти нюансы характеризуют и немецкую основательность во всем, и близость немецкой позиции к китайской. Рассматриваемая книга фактически детально анализирует и верифицирует тезис, встречаемый в литературе, о том, что если раньше Китай следовал правилам глобальной экономики (*rule taker*), то затем стал их менять (*rule changer*), а теперь — формировать (*rule maker*) (Дегтерев и др., 2021, с. 216). Согласно инициативе *Made in China 2025*, Китай планирует стать лидером в том числе в ИКТ нового поколения, робототехнике, новых материалах, судостроении, производстве передового

железнодорожного оборудования, биомедицине и производстве медоборудования (Simon, 2021, p. 108).

Перспективы Китая — активно обсуждаемый вопрос в научном экономическом сообществе. В теоретическом плане отмечается, что для начала перехода глобального лидерства от одной страны к другой стране-претенденту достаточно 80 % «силы» ныне доминирующей страны, а при 120 % «транзит власти» завершается (Дегтерев и др., 2021, с. 212). Причем мы опять имеем дело с преемственностью: еще 60 лет назад основатель теории «властного транзита» А.Ф.К. Органски считал, что вопрос о закономерном выдвигании Китая в мировые лидеры уже решен, — неизвестно только, сколько потребует времени.

Однако явно напрашивается еще один вопрос: чем же объясняется такой успех Китая? Данный вопрос тянет за собой целую цепочку дилемм: Север — Юг, развитие — развивающиеся страны, инновации — традиции, противостояние — сотрудничество, разрушение — создание, технократия — культура. Посмотрим, к какому же выводу приходит в итоге Г. Саймон.

После раскрытия в первом разделе книги концепции «скрытых чемпионов» — истории данной концепции, определения, ее генезиса и положения о важной роли «скрытых чемпионов» в развитии экспорта стран, во втором разделе под заголовком «Скрытые чемпионы и экспортный успех» Г. Саймон обращается к конкретным цифрам. Во-первых, он рассматривает суммарный объем экспорта в 2010—2019 гг. и получает тройку стран, лидирующих с большим отрывом: КНР — 20 917 млрд долл. США, США — 15 420 млрд долл. США, Германия — 13 934 млрд долл. США. У Японии, следующей за ними, экспорт почти вдвое меньше (7 082 млрд долл. США), у Франции (союзника по ЕС) — почти трехкратное отставание (5 590 млрд долл. США). Затем ученый берет показатель подушевого экспорта за аналогичный период и получает бесспорного лидера — Германию — со значением в 168 594 долл. США; у США он составляет 47 383 долл. США, у КНР — 15 039 долл. США (Simon, 2021, pp. 9—10).

В 2019 г. КНР опережала США по обоим показателям, причем по объему экспорта — на целую четверть, что подтверждает выдвинутую гипотезу о смене лидера. По числу «скрытых чемпионов» лидирует Германия (1573), на порядок опережая США и другие страны; Китай (97) уступает США в 3 раза, но опережает Великобританию. При этом Китай ставит серьезные цели развития и выступает с инициативой создания 1000 «скрытых чемпионов», в 2021 г. в КНР была принята программа с бюджетом 1,3 млрд долл. США (Simon, 2021, pp. 27—28, 33).

Третий раздел «Новая игра глобализации» (главы 11—15) посвящен анализу процесса и результатов глобализации, которая выступила главным драйвером восхождения «скрытых чемпионов», и анализу США и Китая как целевых рынков немецких СЧ. Учен прогнозирует, что по размеру ВВП и его росту в первой глобальной лиге к 2030 г. с большим отрывом от остальных будут идти Китай, США и ЕС. Они существенно выиграли от предыдущего этапа глобализации, причем Китай получил наибольший выигрыш с 1990 г. в соотношении с ВВП на душу населения в 1990 г., на порядок опередив США (835 против 52 %) (Simon, 2021, pp. 58, 78, 82).

Главная привлекательность рынка Китая — высокий рост, и это жизненно важно для немецких СЧ, как важен объем рынка США. КНР все чаще предстает в роли инвестора. Уже около 4 тыс. китайских компаний работают в Германии. В 2014—2020 гг. произошло 300 поглощений немецких компаний китайскими, тогда как китайских немецкими — только 60. Китай уже успешен в некоторых высокотехнологичных сегментах. Так, он производит 80 % батарей для электромобилей, 70 % солнечных панелей, уже далеко продвинулся в применении искусственного интеллекта. Стремительно растет использование китайских патентов в Европе и США, из 40 тыс. патентов в сфере ветроэнергетики, зарегистрированных в мире к сентябрю 2019 г., 42 % — китайские (Simon, 2021, pp. 109, 117, 165).

По прогнозам, Азия будет идти впереди в цифровом маркетинге. По числу суперкомпьютеров Китай по состоянию на ноябрь 2021 г. опережает США (173 против 149)¹.

¹ List Statistics // Top 500. URL: <https://www.top500.org/statistics/list/> (accessed: 10.01.2022).

Хотя китайские СЧ еще пока немногочисленные (97), они растут быстрыми темпами, у них намного больше R&D-сотрудников (Simon, 2021, p. 113), то есть у китайских СЧ еще все впереди. По расчетам, сделанным с опорой на данные ЮНКТАД, экспорт высококвалифицированных и технологически интенсивных производств в Китае в 1995—2020 гг. вырос в 32 раза, в то время как у США — в 2 раза². Даже в условиях пандемии Китай показывает впечатляющие результаты в экспорт-ориентированном технологическом развитии: в первом полугодии 2021 г. доля машин и электрооборудования в экспорте достигала 59,2 % (что выше, чем в первом полугодии 2020 г.). Рост экспорта базируется на растущем производстве: в среднем за 2 последних года китайское производство «зеленых» автомобилей, промышленных роботов и интегральных схем выросло более чем на 30 % (Григорьев, 2021, с. 74, 77).

О стремительном развитии Китая свидетельствует и рост его индекса развития человеческого потенциала: согласно данным Программы развития ООН, в 1990—2019 гг. он вырос с 0,499 до 0,761, в то время как у США — с 0,865 до 0,926³.

Четвертый и пятый разделы рецензируемой монографии посвящены ресурсам СЧ в век Китая. Главы 16—19 содержат характеристику новой игры преобразующих сил: бизнес-экосистем, цифровизации, тренда устойчивости и инноваций. В целом книга резюмирует, что будущее «скрытых чемпионов» будет определяться сопричастностью к высшей глобальной лиге (Китай, США и ЕС). Причем Китай заслуживает предельного внимания и как целевой рынок, и как источник новых конкурентов и инноваций. Наличие у компании сильных позиций в США и КНР — обязательное условие для лидерства на мировом рынке. Поскольку планы трансатлантического партнерства США и ЕС не были реализованы (Simon, 2021, pp. 96—97), не происходит и объединения технологического и экспортного потенциала

² Рассчитано по: International merchandise trade // UNCTAD. URL: <https://unctadstat.unctad.org> (accessed: 13.01.2022).

³ Human Development Index Trends, 1990—2019 // UNDP. 2020. P. 348. URL: <http://hdr.undp.org/en/composite/trends> (accessed: 13.01.2022).

«Глобального Севера», поэтому Китай имеет возможность конкурировать с каждым из этих технополюсов по отдельности. Г. Саймон придерживается, как и в предыдущих своих монографиях, позиции *win — win* («выигрывают оба») (нем. *sowie als auch*). Для усиления позиций немецких СЧ для них в одинаковой степени важны рынки и КНР, и США. Чем более доступными будут рынки одной страны для другой, тем на большие уступки пойдут партнеры: от устранения барьеров выигрывают все, в том числе и «скрытые чемпионы».

Таким образом, представленная книга вносит существенный вклад в исследование технологических разрывов и технологических трансферов между развитыми странами

(США, ЕС) и странами «Глобального Юга» (в лице Китая). Монография раскрывает современную исходную ситуацию в развитии высокотехнологичных экспорт-ориентированных компаний в лице «скрытых чемпионов» в странах Юга и Севера (на примере Китая, Германии и других стран), а также анализирует инструменты и условия, имеющиеся у стран Юга и Севера в корпоративном разрезе на примере компаний — «скрытых чемпионов». Это обуславливает высокую теоретическую и практическую значимость книги как для дальнейших исследований в плане расстановки сил на мировой арене, так и для содействия развитию технологий и несырьевого экспорта инновационных и экспорт-ориентированных компаний.

Поступила в редакцию / Received: 14.01.2022

Принята к публикации / Accepted: 18.04.2022

Библиографический список

- Григорьев М. Экономика Китая в первом полугодии 2021 г. // Экономист. 2021. № 9. С. 74—79.
- Дегтерев Д. А., Рамич М. С., Цвык А. В. США — КНР: «властный транзит» и контуры «конфликтной биполярности» // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2021. Т. 21, № 2. С. 210—231. <https://doi.org/10.22363/2313-0660-2021-21-2-210-231>
- Саймон Г. Скрытые чемпионы: уроки 500 лучших в мире неизвестных компаний. Москва : Дело, 2005.
- Levitt T. The Globalization of Markets // Harvard Business Review. 1983. May — June. P. 92—102.
- Simon H. Hidden Champions — Lessons from 500 of the World's Best Unknown Companies. Cambridge : Harvard Business School Press, 1996.
- Simon H. Hidden Champions: The New Game in the Chinese Century. Frankfurt — New York : Campus, 2021.

References

- Degterev, D. A., Ramich, M. S., & Tsvyk, A. V. (2021). U.S. — China: “Power transition” and the outlines of “conflict bipolarity”. *Vestnik RUDN. International Relations*, 21(2), 210—231. <https://doi.org/10.22363/2313-0660-2021-21-2-210-231>
- Grigoryev, M. (2021). Economy of China in the 1st half-year of 2021. *Economist (Russia)*, (9), 74—79. (In Russian).
- Levitt, T. (1983). The globalization of markets. *Harvard Business Review*, (May — June), 92—102.
- Simon, H. (1996). *Hidden champions — lessons from 500 of the world's best unknown companies*. Cambridge: Harvard Business School Press.
- Simon, H. (2005). *Hidden champions — lessons from 500 of the world's best unknown companies*. Moscow: Delo publ. (In Russian).
- Simon, H. (2021). *Hidden champions: The new game in the Chinese century*. Frankfurt — New York: Campus.

Сведения об авторах: Андреева Елена Леонидовна — доктор экономических наук, профессор, руководитель центра региональных компаративных исследований Института экономики УрО РАН; ORCID: 0000-0003-4975-0905; e-mail: andreeva.el@uiec.ru

Ратнер Артем Витальевич — кандидат экономических наук, старший научный сотрудник центра региональных компаративных исследований Института экономики УрО РАН; ORCID: 0000-0001-7173-5328; e-mail: ratner.av@uiec.ru

About the authors: Andreeva Elena Leonidovna — PhD, Dr. of Sc. (Economic Sciences), Professor, Head, Centre of Regional Comparative Research, Institute of Economics of the Ural Branch of RAS; ORCID: 0000-0003-4975-0905; e-mail: andreeva.el@uiec.ru

Ratner Artem Vitalyevich — PhD in Economics, Senior Research Fellow, Centre of Regional Comparative Research, Institute of Economics of the Ural Branch of RAS; ORCID: 0000-0001-7173-5328; e-mail: ratner.av@uiec.ru



DOI: 10.22363/2313-0660-2022-22-2-433-435

Рецензия на книгу :
Bhatia R. India — Africa Relations: Changing Horizons.
New York : Routledge, 2021. 244 p.

Н.А. Медушевский ✉

Российский государственный гуманитарный университет, Москва, Российская Федерация

✉lucky5659@yandex.ru

Для цитирования: Медушевский Н. А. Рецензия на книгу : Bhatia R. India — Africa Relations: Changing Horizons. New York : Routledge, 2021. 244 p. // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 433—435. <https://doi.org/10.22363/2313-0660-2022-22-2-433-435>

Book review:
Bhatia, R. (2021). India — Africa Relations: Changing Horizons.
New York: Routledge, 244 p.

Nikolay A. Medushevsky ✉

Russian State University for the Humanities, Moscow, Russian Federation

✉lucky5659@yandex.ru

For citation: Medushevsky, N. A. (2022). Book review: Bhatia, R. (2021). India — Africa Relations: Changing Horizons. New York: Routledge, 244 p. *Vestnik RUDN. International Relations*, 22(2), 433—435. (In Russian). <https://doi.org/10.22363/2313-0660-2022-22-2-433-435>

В рамках изучения современного глобализирующегося мира все больший интерес исследователей привлекают системы сотрудничества, выстраиваемые «молодыми» участниками международных отношений. Во многом данные системы взаимодействия несут в себе альтернативу господствовавшей до последнего времени однополярной системе во главе с США и открывают путь к созданию нового многополярного миропорядка.

В данной связи научный исследовательский интерес вызывает работа индийского политолога и дипломата Раджива Бхатии *India — Africa Relations: Changing Horizons* (Bhatia, 2021). Название работы можно перевести на русский язык как «Индийско-африканские

отношения: меняющиеся (изменчивые) горизонты».

Прежде чем перейти к обзору данной публикации, увидевшей свет в 2021 г., следует сказать несколько слов о ее авторе. Раджив Бхатия — выдающийся сотрудник *Gateway House*, Индийского совета по глобальным отношениям, который является крупным аналитическим центром по внешней политике Индии, созданном в 2009 г. для привлечения ведущих корпораций и частных лиц Индии к обсуждению и изучению внешней политики страны и ее роли в глобальных делах¹.

Р. Бхатия является специалистом по африканской проблематике. Он долгое время исполнял обязанности Верховного комиссара

¹ About Gateway House // Gateway House. URL: <https://www.gatewayhouse.in/about-us/> (accessed: 29.11.2021).

© Медушевский Н.А., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

Индии в Кении, Южной Африке и Лесото, а также посла Индии в Мьянме и Мексике. В 2012—2015 гг. Р. Бхатия занимал пост генерального директора Индийского совета по международным делам (ICWA) и работал приглашенным научным сотрудником в Институте исследований Юго-Восточной Азии (ISEAS) в 2011—2013 гг. Р. Бхатия является автором таких работ, как «Индия в глобальных делах: перспективы дома Сапру» (Bhatia, 2015) и «Отношения Индии и Мьянмы: Изменение контуров» (Bhatia, 2016).

Новая работа автора посвящена именно индийско-африканским отношениям, что особенно актуально в контексте разворачивающейся сегодня на глобальной арене борьбы за влияние на страны Африки между ведущими мировыми державами.

Индийский исследователь констатирует, что на наших глазах происходит становление и утверждение Африки в качестве важного участника и заинтересованной стороны в глобальных делах, причем если раньше африканские страны выступали преимущественно в качестве объекта международных отношений, то сейчас многие из них приобретают все большую субъектность и начинают проводить самостоятельную политику по взаимодействию с внешними игроками. Одним из таких игроков глобальной политики как раз и выступает Индия, которая с приходом к власти в 2014 г. премьер-министра Нарендры Моди окончательно определилась с геополитическими приоритетами и взяла курс на сближение с целым рядом африканских государств.

Автор книги отмечает, что, несмотря на краткосрочность современного этапа сотрудничества, Индия не начинает свою политику с нуля, так как у обеих сторон существует широкий исторический фон и общее колониальное прошлое, которые определяют вектор взаимодействия и позволяют сосредоточиться на эволюции отношений между Индией и Африкой в контексте первых двух десятилетий XXI в.

В рамках изучения современного взаимодействия Индии с африканскими государствами большое внимание уделяется вопросам конкуренции глобальных игроков за право приоритетного взаимодействия с отдельными

странами континента. В книге подробно исследуется разворачивающаяся международная конкуренция, в которой участвуют такие мощные глобальные субъекты, как ЕС, США и Япония, а также подробно рассматривается растущее влияние Китая на территории всего континента. КНР является глобальным антагонистом Индии и создает трансрегиональные проекты, способные привести к региональной изоляции своего соперника.

Геополитическое усиление КНР и стремление Китая охватить Евразию и Африку системой транзитных маршрутов, наиболее известным среди которых является проект «Пояса и пути», выступает главной причиной обострения противостояния в Африке. «Пояс и путь» предполагает создание трех трансевразийских экономических коридоров: северного (Китай — Центральная Азия — Россия — Европа), центрального (Китай — Центральная и Передняя Азия — Персидский залив и Средиземное море) и южного (Китай — Юго-Восточная Азия — Южная Азия — Индийский океан).

Также Китай работает над созданием проекта «Морского Шелкового пути XXI века», который предполагает обеспечение транзитного маршрута по двум путям: через Южно-Китайское море в Южно-Тихоокеанский регион и из Китая и Европу через Южно-Китайское море и Индийский океан.

Индия де-юре не поддерживает ни один из этих проектов, так как каждый из них в отдельности и они вместе взятые способны изолировать индийскую торговлю и подчинить ее китайским интересам. В этой связи актуализируется борьба между Китаем и Индией за партнеров в бассейне Индийского океана, в том числе и на Африканском континенте.

При этом Китай проводит достаточно агрессивную политику, укрепляя в том числе свою военную инфраструктуру. В качестве примера можно привести военно-морскую базу в Джибути, где базируется 12 000 китайских военных. В то же время Китай предлагает африканским странам-партнерам большие финансовые инвестиции и гибкие и комплексные формы сотрудничества, в числе которых кредиты, строительство инфраструктуры, подготовка кадров и т. д. Китайская региональная

политика находит свое отражение в главе, названной автором «Африкано-китайское танго».

В ответ на активную политику КНР Индия предлагает Африке свой проект Азиатско-африканского коридора роста (*Asia — Africa Growth Corridor*, AAGR), реализуемый совместно с Японией – антагонистом КНР. AAGR направлен на развитие в области здравоохранения и фармацевтики, сельского хозяйства и переработки сельскохозяйственной продукции, борьбы со стихийными бедствиями и повышения квалификации специалистов. Японская сторона заявила, что будет поддерживать и финансировать проекты, даже если они будут осуществляться в Африке индийскими компаниями в сотрудничестве с японскими компаниями.

Кроме сотрудничества с Японией в рамках AAGR Индия с 1990-х гг. разрабатывает свою стратегию для Индийско-Тихоокеанского региона. Ключевой элемент этой стратегии — развитие инфраструктуры в Южной, Юго-Восточной и Восточной Африке. В рамках реализации стратегии реализуется наращивание совместной работы с Японией и США в бассейне Индийского океана, включая такие страны, как Бангладеш, Мьянма, Таиланд и Кения. Об этом Р. Бхатия подробно пишет в главах «Взаимодействие между Индией и Африкой в XXI веке» и «Двусторонние аспекты». В данных разделах ученый детально анализирует континентальные, региональные и двусторонние аспекты отношений между Индией и Африкой и предлагает дорожную

карту для укрепления и углубления сотрудничества в предстоящее десятилетие.

Отметим, что сразу после публикации рецензируемая монография Р. Бхатии получила много положительных отзывов как в самой Индии, так и за ее пределами. В числе тех, кто высоко оценил книгу, были посол Кении в Индии д-р Моника Джума, бывший министр иностранных дел правительства Индии Лалит Мансингх, ведущий индийский ученый в области африканских исследований и международных отношений Раджен Харше и Исполнительный директор Южноафриканского института международных отношений (SAIIA) Элизабет Сидиропулос.

Подводя итог нашей рецензии, необходимо отметить, что монография Р. Бхатии является не только интересной, но и крайне значимой публикацией, поскольку обобщает ценный опыт индийско-африканской и региональной политики, который практически не известен российским исследователям и присутствует в российском научном пространстве лишь фрагментарно. Вместе с тем данный опыт важен в контексте реализации Индией глобальной политики, а также политики в области сотрудничества с Россией, которая, в свою очередь, также имеет выраженные интересы на Африканском континенте. Именно поэтому монография Р. Бхатии обязательно заинтересует российских читателей и может быть полезна для подготовки университетских курсов по региональной и международной политике и при проведении комплексных научных исследований.

Поступила в редакцию / Received: 18.12.2021

Принята к публикации / Accepted: 18.04.2022

Библиографический список / References

- Bhatia, R. (2015). *India in global affairs: Perspectives from Sapru house*. New Delhi: KW Publishers.
 Bhatia, R. (2016). *India — Myanmar relations: Changing contours*. London: Routledge India.
 Bhatia, R. (2021). *India — Africa relations: Changing horizons*. New York: Routledge.

Сведения об авторе: Медушевский Николай Андреевич — доктор политических наук, профессор кафедры культуры мира и демократии Российского государственного гуманитарного университета; e-mail: lucky5659@yandex.ru

About the author: Medushevsky Nikolay Andreevich — PhD, Dr. of Sc. (Political Sciences), Professor, Chair of Peace Culture and Democracy, Russian State University for the Humanities; e-mail: lucky5659@yandex.ru



DOI: 10.22363/2313-0660-2022-22-2-436-438

Рецензия на книгу :
Россия и Африка. Документы и материалы. 1961 — начало 1970-х /
отв. ред. С.В. Мазов, А.Б. Давидсон.
Москва : Политическая энциклопедия, 2021. 1006 с.

Ныгусие В.М. Кассае  

Российский университет дружбы народов, Москва, Российская Федерация
[✉kassae-nv@rudn.ru](mailto:kassae-nv@rudn.ru)

Для цитирования: Кассае Ныгусие В. М. Рецензия на книгу : Россия и Африка. Документы и материалы. 1961 — начало 1970-х / отв. ред. С.В. Мазов, А.Б. Давидсон. Москва : Политическая энциклопедия, 2021. 1006 с. // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 436—438. <https://doi.org/10.22363/2313-0660-2022-22-2-436-438>

Book review:
Mazov, S. V., & Davidson, A. B. (Eds.). (2021). Russia and Africa.
Documents and Materials. 1961 — early 1970s.
Moscow: Politicheskaya entsiklopediya publ., 1006 p. (In Russian)

Nigusie W.M. Kassaye  

Peoples' Friendship University of Russia, Moscow, Russian Federation
[✉kassae-nv@rudn.ru](mailto:kassae-nv@rudn.ru)

For citation: Kassaye, Nigusie W. M. (2022). Book review: Mazov, S. V., & Davidson, A. B. (Eds.). (2021). Russia and Africa. Documents and Materials. 1961 — early 1970s. Moscow: Politicheskaya entsiklopediya publ., 1006 p. (In Russian). *Vestnik RUDN. International Relations*, 22(2), 436—438. (In Russian). <https://doi.org/10.22363/2313-0660-2022-22-2-436-438>

«Мы выражаем Вашему Превосходительству от своего имени и от имени народов Эфиопии восхищение и безграничную радость, которые чувствует каждый из нас. Эта победа, несущая нам окончание самой дикой тирании, которую когда-либо знал мир, привела нас к преддверию эпохи большего счастья и большей справедливости для всех народов, которым угрожало уничтожение. Мы хотим использовать данный случай для того, чтобы напомнить Вашему Превосходительству, что никогда ни

Мы, ни народы Эфиопии не забывали о поддержке, оказанной нам Советским Союзом в те мрачные дни 1935 г., когда мы поставили наше дело на решение Лиги Наций»¹. Эти слова главы Эфиопии императора Хайле Селассие I председателю Совета Министров СССР Иосифу Сталину от 10 мая 1945 г. являются подтверждением тому, что СССР не только оказывал дипломатическую поддержку, но и сыграл большую роль в освобождении Африканского континента от колониализма.

¹ Россия и Африка. Документы и материалы. XVIII в. — 1960 г. Т. 2: 1918—1960 гг. Москва : ИВИ РАН, 1999. С. 47—48.

© Кассае Ныгусие В.М., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

Советское правительство поставило на обсуждение XVI сессии Генеральной Ассамблеи ООН вопрос о предоставлении независимости колониальным странам и народам. Именно под дипломатическим давлением Советского Союза была принята Декларация о предоставлении независимости колониальным странам и народам, провозгласившая необходимость покончить с колониализмом и любой сегрегацией и дискриминацией. Несмотря на возражения колониальных держав, в частности Великобритании и Франции, документ был утвержден на сессии Генеральной Ассамблеи ООН в 1960 г.

Книга «Россия и Африка. Документы и материалы. 1961 — начало 1970-х» является продолжением двухтомника «Россия и Африка. Документы и материалы. XVIII век — 1960 г.» (Россия и Африка..., 1999). Документы сборника охватывают период с 1961 по 1973 г. Их тематика довольно широка, она отражает расширение и усложнение советско-африканских связей, новые процессы в независимых африканских странах и в мире. Представлены информационные и аналитические материалы о проблемах советской экономической помощи и пропагандистской работы, советско-китайском соперничестве в Африке, военных переворотах, теориях и практике африканского социализма, внутренних вооруженных конфликтах в Демократической Республике Конго и Нигерии.

Объем сборника внушителен: 409 документов, 63 печатных листа, 1006 страниц. В книгу вошли ранее не публиковавшиеся документы о советско-африканских связях и отношениях с 1961 до начала 1970-х гг. из фондов Архива внешней политики Российской Федерации (АВП РФ), Российского государственного архива новейшей истории (РГАНИ), Государственного архива Российской Федерации (ГА РФ), Государственного архива Свердловской области (ГАСО). Коллектив составителей насчитывает 11 человек, в основном сотрудники Центра африканских исследований Института всеобщей истории РАН. В редколлегия вошли С.В. Мазов, А.Б. Давидсон (ответственные редакторы), А.С. Балезин и А.В. Воеводский.

Документы сгруппированы по тематическому и географическому принципам,

охватывают все основные регионы Африки южнее Сахары и отдельные страны, у которых сложились с СССР наиболее типичные и репрезентативные отношения.

Первые четыре раздела — тематические. Раздел I «Основные направления сотрудничества СССР со странами Африки» включает документы по общим вопросам и проблемам советско-африканских связей, советскому видению ситуации в Африке. В частности, представлены источники о направлении групп советской молодежи на работу в страны Африки, помощи КПСС левым организациям, культурных и научных связях СССР со странами Африки, а также организации издания учебных пособий и брошюр для распространения в странах Азии, Африки и Латинской Америки. Аналитический характер носят отчет о служебной поездке по странам Африки в 1961 г. первого заместителя председателя правления Агентства политических новостей (АПН) С.И. Беглова и записка в ЦК КПСС директора Института Африки Академии наук СССР В.Г. Солодовникова «Причины и уроки государственных переворотов в Африке» (март 1966 г.).

В разделе II «Африканцы в России» собраны документы о жизни африканских студентов в СССР. В числе источников: справка заместителя министра высшего и среднего специального образования М.А. Прокофьева об обучении иностранных студентов в советских вузах и состоянии воспитательной работы с ними; предложения сотрудников ЦК КПСС о подготовке в СССР квалифицированных кадров для развивающихся стран; информация председателя Всесоюзного центрального совета профессиональных союзов (ВЦСПС) В.В. Гришина о работе курсов ВЦСПС для профсоюзных активистов стран Азии, Африки и Латинской Америки; материалы об участии африканских студентов во Всеафриканской конференции студентов в Белграде, документы об инцидентах между африканцами и советскими гражданами.

Раздел III «Россияне в Африке» посвящен советским специалистам, работавшим в странах Африки. Представленные документы раскрывают проблемы их повседневной жизни, условия труда, государственные меры, направленные на улучшение их материального положения, политической и языковой подготовки.

Значительную часть IV раздела «Формирование взаимных представлений» составляют отчеты о поездках в Африку делегаций СССР и отдельных чиновников, впечатления работавших в Африке дипломатов и других советских специалистов. Эти материалы открывают реальную Африку, о которой нельзя было узнать из советской печати. Отчеты о приеме делегаций из африканских стран показывают характер представлений африканцев о Советском Союзе. Узнавание друг друга на межличностном уровне продемонстрировано на примере переписки между южноафриканкой Г. Кокран и сотрудником Союза советских обществ дружбы (ССОД) В. Панкратьевым.

Три раздела — региональные. Характер региональных документов обусловлен спецификой связей между странами Западной, Восточной, Центральной Африки и Юга континента с Советским Союзом.

Главные темы V раздела «Западная Африка» (Гана, Гвинея, Либерия, Мали, Нигерия, Сенегал) — проблемы отношений с первыми в Африке странами социалистической ориентации (Гана, Гвинея, Мали) и советская позиция в отношении первой масштабной и кровопролитной гражданской войны в Африке (Нигерия).

В VI разделе «Северо-Восточная и Восточная Африка» приведены документы о становлении и развитии отношений с Занзибаром, Кенией, Мадагаскаром, Сомали, Танганьикой, Угандой и Эфиопией.

Ключевой сюжет VII раздела «Центральная Африка» (Ангола, Конго (Леопольдвиль), с 1 августа 1964 г. — Демократическая Республика Конго, Конго (Браззавиль), с 3 января 1970 г. — Народная Республика Конго) находится конголезский кризис (1960—1965). Представленные документы раскрывают характер участия СССР в схватке за «сердце Африки» и причины его проигрыша. Ангольские документы показывают, с какими проблемами сталкивалось советское руководство при выборе союзников среди движений, ведущих борьбу за независимость Анголы.

Раздел VIII «Южная и Юго-Восточная Африка» содержит документы, относящиеся к Ботсване, Замбии (до 24 октября 1964 г. — Северная Родезия), Лесото (до 4 октября 1966 г. — Басутоленд), Мозамбику, Намибии (до 1968 г. — Юго-Западная Африка), Свазиленду, Южной Родезии и Южно-Африканской Республике (до 31 мая 1961 г. — Южно-Африканский Союз). Основная часть документов посвящена советской помощи национально-освободительным движениям, боровшимся против режима апартеида в ЮАР, правления белого меньшинства в Южной Родезии и колониального режима Португалии в Мозамбике.

Сборник вводит в научный оборот большой массив ранее не публиковавшихся документов о советско-африканских связях и станет ценным подспорьем для исследователей этой темы.

Поступила в редакцию / Received: 18.01.2022
Принята к публикации / Accepted: 18.04.2022

Библиографический список

- Россия и Африка. Документы и материалы. 1961 — начало 1970-х* / отв. ред. С. В. Мазов, А. Б. Давидсон. Москва : Политическая энциклопедия, 2021.
- Россия и Африка. Документы и материалы. XVIII в. — 1960 г.* Т. 2: 1918—1960 гг. / отв. ред. А. Б. Давидсон, С. В. Мазов. Москва : ИВИ РАН, 1999.

References

- Davidson, A. B., & Mazov, S. V. (Eds.). (1999). *Russia and Africa. Documents and materials. 18th — 1960s*. Vol. 2: 1918—1960. Moscow: IVI RAN publ. (In Russian).
- Mazov, S. V., & Davidson, A. B. (Eds.). (2021). *Russia and Africa. Documents and materials. 1961 — early 1970s*. Moscow: Politicheskaya entsiklopediya publ. (In Russian).

Сведения об авторе: Кассая Ныгусие Вольде Михаэль — доктор исторических наук, профессор кафедры теории и истории международных отношений Российского университета дружбы народов; ORCID: 0000-0002-2792-6634; e-mail: kassae-nv@rudn.ru

About the author: Kassaye Nigusie Wolde Michael — Dr. of Sc. (History), Professor, the Department of Theory and History of International Relations, Peoples' Friendship University of Russia (RUDN University); ORCID: 0000-0002-2792-6634; e-mail: kassae-nv@rudn.ru