RUDN Journal of World History
ISSN 2312-8127 (print), ISSN 2312-833X (online)
Вестник РУДН. Серия: ВСЕОБЩАЯ ИСТОРИЯ
2022 Vol. 14 No. 2 197–210
http://journals.rudn.ru/world-history

ВОСТОК-ЗАПАД: КОНТАКТЫ И ПРОТИВОРЕЧИЯ
EAST AND WEST: CONTACTS AND CONTRADICTIONS

DOI: 10.22363/2312-8127-2022-14-2-197-210

Научная статья / Research article

Китайские концепции и возможности в информационной войне: соперничество КНР и США в киберпространстве

Е.Ю. Каткова✉, А.С. Юнюшкина

Российский университет дружбы народов,
117198, *Российская Федерация*, *Москва*, *ул. Миклухо-Маклая*, *д. 6*
✉katkova-eyu@rudn.ru

Аннотация. В статье авторы затрагивают возникающие угрозы информационной безопасности, имеющиеся между двумя крупными державами – Китаем и США. Информационное противостояние между этими странами носит стратегический характер, истоки которого уходят в киберпространство. В статье анализируются различные подходы специалистов из КНР и США к политике по оказанию противодействия данным угрозам. Также авторы рассматривают формы и методы, необходимые для урегулирования возникающих вызовов и угроз в информационной сфере. Жесткое соперничество Китая и США, которые являются самыми крупными экономиками и больше всего инвестируют средства на развитие военно-технического комплекса, будет явно отражаться в информационной сфере.

Ключевые слова: информационная война, кибербезопасность, КНР, США, информационные технологии, стратегии, потенциал

История статьи: Поступила в редакцию: 20.05.2021. Принята к публикации: 27.10.2021

Для цитирования: *Каткова Е.Ю.*, *Юнюшкина А.С.* Китайские концепции и возможности в информационной войне: соперничество КНР и США в киберпространстве // Вестник Российского университета дружбы народов. Серия: Всеобщая история. 2022. Т. 14. № 2. С. 197–210. https://doi.org/10.22363/2312-8127-2022-14-2-197-210

Chinese Concepts and Opportunities in Information Warfare: China–US Rivalry in Cyberspace

Evgeniya Yu. Katkova✉, Anna S. Yunyushkina

Peoples' Friendship University of Russia (RUDN University),
6 Miklukho-Maklay St, *Moscow*, *Russia*, *117198*
✉katkova-eyu@rudn.ru

Abstract. The research is devoted to the emergence of threats to information security and competition in cyberspace between the two largest powers – China and the United States. Over

the past ten years, China has been actively developing offensive cyber capabilities, turning into a state with a combat- ready and modern army. Its technological level is behind the United States in many areas, but Beijing is rapidly closing the gap. Today, the information confrontation between these countries is of a strategic nature. Both China and the United States are investing large sums of money in the development of cyber technologies. The authors examine the different approaches of China and the United States to the methods of waging information wars and countering various challenges and threats in cyberspace. In conclusion, the authors come to the opinion that China will actively develop information technologies and build up its strategic potential in this area in the near future, which will lead to tougher competition among major powers in cyberspace.

Keywords: information war, cybersecurity, China, USA, information technology, strategic potential

Article history: Received: 20.02.2021. Accepted: 27.10.2021.

For citation: Katkova EYu., Yunyushkina AS. Chinese Strategies and Opportunities in Information Warfare: China–US Rivalry in Cyberspace. *RUDN Journal of World History*. 2022;14(2):197–210. https://doi.org/10.22363/2312-8127-2022-14-2-197-210

Введение

В последние годы Китайская Народная Республика продемонстрировала большой интерес к методикам ведения информационной войны. В основе китайских постулатов по ее ведению лежат благоприятные условия для «восстановления своего законного места ведущей державы в Азии» [1. С. 387], а также дальнейшего выживания и процветания своего народа. Информационная война в целом не является новым явлением и практиковалась с древности, в том числе такими великими полководцами, как Ксеркс и Александр Великий [2. С. 8]. Военные ученые относят ее происхождение к трудам китайского стратега, жившего в V в. до нашей эры, Сунь-цзы. С древних времен в Китае существовала сфера информационного противоборства, которая дала начало особой философии, заключающейся в дезинформационном воздействии на окружающий мир, а также в своеобразном стиле мышления человека. Большинство положений данной философии было представлено в учениях военного теоретика Сунь-цзы, работы которого постоянно переводятся на иностранные языки [3. С. 38]. Для Китая в тот период времени использование дезинформации при ведении военных действий было весьма актуально, поэтому работы данного стратега являлись важным источником полезной информации. В настоящее время произведения древнекитайского стратега продолжают пользоваться большим интересом, активно используются в качестве учебных пособий для обучения персонала спецслужб, государственных и иных организаций, сфера деятельности которых тесно связана с кибербезопасностью. Распространение новых технологий и Интернета позволило странам практиковать современные формы информационной войны друг против друга инновационными способами [4. С. 444].

На сегодняшний день известно, что многие страны, в том числе демократические, используют информацию для достижения стратегических целей.

И демократии, и автократии стремятся развивать свои кибертехнологии, чтобы получить преимущество в оборонительных и наступательных возможностях. Однако в этой области автократии находятся в более выигрышном положении. Во-первых, в демократических странах гражданское общество требует прозрачности при принятии решений и при формировании бюджета, что значительно ограничивает военные круги в финансовых вопросах. Во-вторых, оборонительные технологии у демократий также менее развиты, в частности, дезинформация легко проникает в национальные сегменты Интернета благодаря свободе слова, что делает очень трудными попытки найти и заблокировать вредоносные сообщения или фэйки, проникающие через рекламу и соцсети. В то время как автократии либо уже выработали механизмы для регулирования Интернета, в частности китайский «Золотой щит» (金盾工程), либо стремятся к контролю путем совершенствования национального законодательства в этой сфере. Таким образом, у Китая есть сравнительное преимущество перед США и другими западными странами в оборонительных и наступательных технологиях ведения информационной войны.

Блестящие достижения США в сфере развития информационных технологий в конце XX в. привело к тому, что Китай начал проводить политический курс, направленный на разработку стратегий для ведения информационной войны.

В прошлые десятилетия в КНР прошла военная модернизация, которая вызвала озабоченность у международного сообщества, поскольку Китай сконцентрировался на развитие сетевых сил, а именно: запустил программу по ведению разработок в области тактики ведения информационной войны, которые предполагают наличие специальных подразделений и специально обученных кадров, обладающих необходимыми знаниями навыками в области информационных технологий и передовых систем [5. P. 100]. Как правило, подготовка таких специалистов происходит в государственных академиях, университетах и специальных учебных заведениях. Большое внимание руководство КНР уделяет вопросу привлечения молодых специалистов в сферу информационных технологий. Увеличивающаяся с каждым годом численность пользователей интернет-пространства в Китае позволяет определить наиболее активных и продвинутых любителей. Кроме того, для поддержания обороноспособности своей страны Пекин, в отличие от демократических стран, может использовать значительные ресурсы и тратить огромные средства на разработку современных доктрин ведения информационной войны [6. С. 63]. Быстрое развитие военных технологий превращает КНР в одного из глобальных лидеров ведения информационной войны [3. С. 40, 68, 73]. Китай рассматривает информацию в качестве центрального инструмента государственной и военной мощи [7. С. 56]. Благодаря огромному успеху в разработке и внедрению информационных технологий, стремительным изменениям ядерного оружия, баллистических ракет и космических инноваций КНР имеет все шансы в ближайшее время выйти на передней план по программам проведения информационных войн.

Соперничество Китая и США в информационной сфере

В 1997 и 1999 гг. американские военные испытали на себе первые атаки китайских хакеров, что заставило правительство США задумать о реальной угрозе национальной безопасности со стороны КНР [8. С. 81]. Серия атак на гражданские и военные базы США оказались неожиданными для Центрального американского командования и управления, что вызвало обеспокоенность в самых высоких политических кругах. Сегодня Китай применяет информационные атаки в целях обеспечения безопасности в Юго-Восточной Азии, регионе, который также занимает важное место во внешней политике США. Особое место информационная безопасность стала играть в свете последних событий в регионе, в частности после начала конкуренции КНР и США за влияние в Азии.

С начала XXI в. в отношении некоторых крупных правительственных систем США были предприняты крупные кибератаки со стороны Китая. По мнению ряда американских специалистов, данные атаки тщательно готовились и разрабатывались благодаря полученной информации от разведывательных служб. Целью данных атак были сети Интернета интересующих объектов инфраструктуры и поиск слабых и уязвимых мест [9. С. 12]. Для эффективности кибератак по оборонным и промышленным учреждениям США Пекин прибегает к использованию технического оборудования, находящегося под непосредственным контролем Народно-освободительной армии Китая (НОАК). Вашингтон полагает, что руководство Китая продолжит проводить операции по получению не только данных оборонного и научно-технического характера, но и сконцентрируется на сборе развединформации политического и экономического характера, касающейся коммерческих и неправительственных организаций, что находится под юрисдикцией министерства государственной безопасности КНР [9. С. 7]. Дополнительно необходимо отметить широкий масштаб кибершпионажа со стороны Китая, который нацелен на государственный и частный сектора США. Например, американская компания AMSC подверглась кибератаке со стороны КНР, направленной на получение программного обеспечения для дальнейшего применения в государственном предприятии Sinovel, что заметно сказалось на доходной стороне американской компании [10. С. 48]. Промышленному кибершпионажу со стороны Китая также подверглась и канадская телекоммуникационная компания Nortel [11. С. 50]. Быстрые темпы экономического развития КНР позволяют Пекину наращивать эффективность промышленного шпионажа против западных стран.

С 2010-х гг. соперничество Китая и США в информационном пространстве продолжает увеличиваться, что может привести к более «горячему» конфликту, который повлияет на современную международную ситуацию. В 2010 г. США обвинили Китай во взломе электронных ящиков правозащитников, что привело к тому, что к 2013 г. начались жесткие взаимные обвинения со стороны официальных лиц двух государств. В марте 2013 г. президент США Б. Обама выступил со специальным распоряжением,

касающееся процедур государственных закупок высокотехнологических решений. По данному распоряжению Госдепартамент США запрещал сотрудничество с Китаем в сфере закупок IT-оборудования для организаций государственного сектора [12]. Это распоряжение вызвало недовольство как внутри США, так и за рубежом. В результате значительные убытки понесли производители, которые напрямую зависят от производственных мощностей Китая, а именно IT-гиганты, такие, как Apple, Dell, HP и т.д. Кроме того, пострадал и сам Китай. Руководство Китая выразило протест против подобных действий со стороны президента США, так как выдвинутые подозрения в отношении китайских компаний не имеют никаких оснований, а значит данная политика больше напоминает нерыночные методы протекционизма [13. С. 312].

Весной 2013 г. Минобороны США выступило с докладом перед Конгрессом «Военный и безопасный потенциал КНР в 2013 г.», в содержании которого обвинило правительство Китая и НОАК в проведении враждебных кибератак по Министерству обороны США и другим ключевым американским учреждениям. КНР активно применяет компьютерные технологии для поддержки разведывательной деятельности, которая направлена против дипломатических организаций и учреждений США, экономического и индустриального секторов обороны [14. С. 36]. Американское руководство считает, что Китай пытается установить контроль над интернет-пространством в целях расширения своего «цифрового суверенитета». В мае 2013 г. на Азиатском саммите по безопасности в Сингапуре тогдашний министр обороны США Ч. Хейгл заявил о том, что количество кибератак со стороны КНР по объектам военного и правительственного назначения постоянно увеличивается [15]. На данное заявление директор Центра китайско-американских отношений в сфере обороны, созданный при Академии военных наук НОАК генерал-майор Яо Юньчжу ответил, что Вашингтон постоянно наращивает военное присутствие в Азиатско-Тихоокеанском регионе, тем самым ставит под вопрос китайско-американского доверия [16].

Таким образом, становится понятно, что Китай и США в открытой форме признают вопросы информационной войны и классических форм военного присутствия, которые играют важное место в системе региональной и глобальной безопасности. КНР с каждым годом совершенствует и развивает стратегию ведения сетевой информационной войны, что оказывает непосредственное влияние на политику Соединенных Штатов [5. С. 110].

Концепции Китая по ведению информационной войны

Концепция «Информационной войны» возникла в середине 90-х гг. XX в. в научных и научно-исследовательских кругах США в качестве объекта для обеспечения интеллектуальной безопасности государства. Постепенно «интеллектуальная лихорадка» охватила и политическое руководство Китая, в результате чего начались обширные разработки по обеспечению информационной безопасности [17. С. 440]. Пекин считает, что информация и информационная

безопасность имеет важное значение для выживания КПК, в связи с чем доминирование в этой области может помочь это обеспечить. Никто не мог ожидать от Китая такого быстрого подъема в данной области, так как не было ни одного опубликованного заявления со стороны Пекина, который в то время активно занимался секретными разработками для поддержания национальной безопасности. Таким образом, можно говорить о возрастающем интересе Китая к тактикам и инструментам информационной войны и триумфальном завершении информационной революции [17. С. 426].

Китайская концепция сетевой войны открывает для китайского руководства и военных специалистов дальнейшие перспективы и возможности ведения работ по созданию и внедрению новейших образцов технологий. Китай время от времени организует собрания по обсуждению методов ведения информационной войны [18. С. 312], а военные специалисты КНР разрабатывают необходимые теоретические концепции для ее успешного проведения [19. С. 280].

В настоящее время КНР встал на путь поиска информационного превосходства. Китайцы ведут разработки возможностей применения технологий ведения информационной войны для достижения своих политических целей. Это не является прямой угрозой для национальной безопасности США, но ставят Вашингтон в уязвимое положение [19. С. 281].

К основным последствиям информационной революции в Китае можно отнести: во-первых, то, что Пекин признает значение высокотехнологичных инноваций и новых информационных технологий; во-вторых, Пекин намерен стать крупной политической и экономической державой, а также прочно укрепить свои позиции на международной арене. Стоить отметить, что руководство КНР придает важное значение экономическому развитию страны, которое является высшим национальным и государственным приоритетом в информационно-экономической сфере; в-третьих, китайские специалисты верят, что благодаря постоянно растущей национальной мощи Китай продолжит удерживать лидирующие позиции среди ведущих игроков многополярного мира; наконец, способность успешно конкурировать экономически и вести высокотехнологическую войну станут основными национальными компонентами силы и мощи Китая [6. С. 65].

Стоит отметить, что информационные войны способствуют компенсации качества и количества вооруженных технологий в Китае, так как методы ведения информационной войны позволяют китайскому руководству вести отдаленную и засекреченную войну с сильнейшими военными державами, такими как США и Россия [20. С. 300]. В основе ведения информационных войн в Китае лежат неортодоксальные методы и возможности, которые позволяют избежать нападений и атак со стороны противника. Китай находится в постоянном процессе разработки тактик, направленных на сдерживание и обеспечение победы по отношению к сильнейшим державам. По оценкам некоторых специалистов, у Пекина есть большой потенциал для достижения превосходства над США в информационной сфере [21]. Китай имеет возможность атаковать весьма уязвимые инфраструктурные объекты США или оказывать

влияние на внутриполитические процессы, тем самым ослабляя и подрывая позиции Америки на международной арене. Мысли Мао Цзэдуна по ведению войны, используя слабости в целях достижения победы над сильным противником, до сих пор имеют значительное влияние на умы высших китайских военных [22. С. 899]. Китайские специалисты также считают, что информационная война является своеобразной ареной, на которой определяется верховенство среди мировых держав. Правительство Китая верит, что информационная война способствует быстрому наращиванию военной мощи Поднебесной [18. С. 313].

Военное превосходство над США рассматривается в Китае как главный ориентир для преодоления и решения всех проблем в информационном и военном плане. Китай уверен, что новые информационные технологии значительно повысят производительную мощность имеющегося оборудования без весомых издержек. К примеру, такие средства сбора информации, как спутники и связанные с ними системы разведки, требуют существенных финансовых вложений, поэтому, за последние два десятилетия Пекин проводит рациональную экономическую политику в целях стабильного развития информационных технологий.

Подход китайского руководства к определению информационной безопасности значительно расходится с западным пониманием смысла обеспечения кибербезопасности. Например, западный подход существенно противоречит китайскому в отношении степени открытости глобальной сети [23. С. 130]. Жесткий контроль Интернета в КНР нацелен на блокирование дальнейшего распространения нежелательной информации внутри государства, а также на предотвращение поступления тайной информации за пределы страны. Благодаря ограничению доступа основных социальных и поисковых систем руководство КНР также контролирует информационный поток и обмен между пользователями глобальной сети. В США термин «кибербезопасность» (cybersecurity) подразумевает главным образом безопасность систем глобальной сети – Интернета. В КНР под данным термином подразумевается «информационная безопасность» (信息安全), которая направлена на борьбу с распространением нежелательной информации. Наличие весомой разницы в подходах к определению термина двух государств значительно осложняет ведение переговоров между ними [8. С. 72].

Китайские аналитики возлагают на информационную войну большие надежды и разделяют ее на две категории, а именно на развитие наступательных и оборонительных возможностей ведения информационной войны [19. С. 283]. К основным методам ведения наступательных операций относятся прямые атаки по информационным системам противника, что парализует и ослабляет систему командования и управления неприятеля [24]. Кроме того, важным инструментом здесь является шпионаж. Сейчас он стал излюбленным методом сбора информации как государственными, так и негосударственными субъектами, в частности спецслужбами [25. С. 445]. Об этом свидетельствуют многочисленные случаи кражи и передачи американской интеллектуальной собственности Китаю для продвижения технологических

разработок как в гражданской, так и в военной сфере [26]. Только за один 2012 г. США оценили убытки, понесенные вследствие кибершпионажа, примерно в 338 млрд долл. США [27. С. 45].

С каждым годом Китай все больше уделяет внимания разработке потенциальных стратегий для успешного ведения информационной войны. Сущность этих стратегий заключается в повышении устойчивости к помехам, усиление защиты от всевозможных атак. Защита собственных информационных платформ и обеспечение нормального функционирования систем становятся одинаково важными компонентами оборонительной политики КНР [21].

Китайское руководство полагает, что использование наступательных и оборонительных операций в ходе проведения информационной войны требует наличия проверенной и эффективной системы управления [8. С. 78]. Конечный результат информационной войны напрямую зависит от командования и управления, которые затрагивают большинство информационных операций, регулируют общую ситуацию. Любая допущенная ошибка здесь ставит под угрозу всю информационную систему. Поэтому вопрос слаженного командования и управления требует повышенного внимания [24]. Один из главных компонентов успешности информационной войны заключается в получении своевременной информации и о реальной ситуации в стране неприятеля для обеспечения собственной безопасности [6. С. 64]. На первых этапах ведения информационной войны необходимо лишить противника способности приобретать, обрабатывать и передавать данные, при этом необходимо обеспечивать защиту собственных информационных систем. К примеру, комплекс систем управления направлен на обеспечение точности ударов, на проведение радиоэлектронной борьбы для выведения из строя атакующих вражеских систем [6. С. 65]. Для поддержания эффективного командования и управления необходимо применять широкий спектр информационных технологий, которые отличаются высокой степенью надежности при совершении дистанционного зондирования и разведки. Очевидно, что дальнейшее применение получат фотографии высокого разрешения, полученные с систем спутникового наблюдения, инфракрасных систем обнаружения, беспилотных самолетов-разведчиков и т.д. [17. С. 37, 98, 201]. Таким образом, к основным инструментам наступательного и оборонительного ведения информационной войны в Китае относятся: физическое уничтожение; кибершпионаж; доминирование электромагнитного спектра; компьютерная сетевая война; психологическая манипуляция [19. С. 284].

Можно также выделить основные аспекты ведения информационной войны. Китайское правительство подчеркивает важность в первую очередь точности нанесения удара по противнику [18. С. 284]. Скрытное оружие сможет выполнять точные удары, которые осуществляются с помощью звуковых и электрических волн, видимого света и инфракрасных лучей. Китайские аналитики согласны, что соревнования за электромагнитный спектр станет важнейшим этапом информационной войны, целью которой станет преобладание над противником в использовании электронного оборудования [18. С. 110, 201, 286]. Постепенно микроэлектроника станет ключевой технологической

областью для инвестиций. Китайские специалисты утверждают, что все более разнообразные формы приобретает сеть компьютерных войн, которые могут проявлять себя как в кибератаках, так и в хакерских войнах. Аналитики рассматривают виртуальную войну как инструмент ложных команд с целью обмана вражеских сил [8. С. 82]. Китайские военные активно проявляют себя в виртуальном моделировании реальных боевых действий.

Другим широко распространенным методом информационной войны является психологическая война, которая подразумевает распространение дезинформации для оказания разрушительного влияния на эмоциональное и физическое здоровье людей, что приводит к заметному ослаблению противника. В ходе проведения психологической войны применяются такие инструменты, как пропаганда СМИ; распространение бумажных листовок; рассылка спам-информации на адреса электронной почты и в социальные сети. В Китае имеются разработки технологий в сфере дистанционного зондирования и проведения разведки [19. С. 284]. Ведутся работы по внедрению фотоэлектронных технологий, которые будут широко применяться в будущем. Данные технологии включают в себя получение более четких фотоснимков; повышение скорости для передачи информации; наличие компактных и мелкогабаритных размеров у оборудования фотоэлектронных систем.

Китай также активно развивает космическую отрасль, наращивает производственные мощности для эффективного обнаружения сил противника [20. С. 300]. Военнослужащие НОАК Китая участвуют в совместных работах с ведущими специалистами в области военного картографирования, дистанционному зондированию и спутниковой навигации [21].

Исходя из интереса Китая к ведению информационной войны, можно говорить о том, что КНР выделяет значительные средства на создание и приобретение современных информационных технологий для того, чтобы создать мощную информационную военную силу. Активное продвижение Китая в космической отрасли позволит создать современную и эффективную разведывательную систему, которая станет значимым компонентом военных сил КНР. Более того, кроме новых технологий информационная война станет подспорьем для политики и стратегий КНР [8. С. 80]. Китай стремится к достижению своих политических целей мирными методами, исключая реальное вооруженное столкновение. Во многих действиях Китая методы информационный войны являются инструментами предотвращения конфликтов путем нанесения ударов по жизненно важным точкам противника, а именно: командованию и управлению информационными системами. По словам некоторых американских специалистов, «одержимость» Китаем информационными технологиями предоставляет собой наиболее опасный и непредсказуемый вызов для безопасности США [21]. Если взять во внимание конфликты на Тайване, то можно проследить следующее: Пекин использовал методы информационной войны для задерживания развертывания американских военных сил на Тайване. Американские войска хотя и обладали высокотехнологичным оборудованием, не смогли предотвратить взломы ПК и ослабление информационных систем. Тем самым была проведена задержка прибытия американских

военных кораблей к берегам Тайваня, а со стороны КНР началось масштабное развертывание комплекса баллистических ракет малой дальности в направлении скопления американских военных структур [24].

Китай также использовал всевозможные виды информационной войны в период предвыборной кампании и президентских выборов на Тайване в 2019–2020 гг. В частности, хакеры и боты распространяли дезинформацию через социальные сети, например, Facebook (21.03.2022 года Тверской районный суд г. Москвы удовлетворил иск Генпрокуратуры РФ и признал деятельность соцсетей Instagram и Facebook, принадлежащих Meta, экстремистской, запретив их работу в России), сервисы микроблогов Weibo и популярные чат-приложения, такие как Line. КНР также усилила пропаганду через тайваньские СМИ, купленные китайскими магнатами [29]. Стоит отметить эффективность этих действий. По данным различных опросов общественного мнения, прокитайский кандидат, представитель партии Гоминьдан, Хань Гоюй достаточно длительное время лидировал в рейтингах, однако события в Гонконге спутали карты КНР, позволив выиграть представителю Демократической прогрессивной партии – Цай Инвэнь (рис. 1).

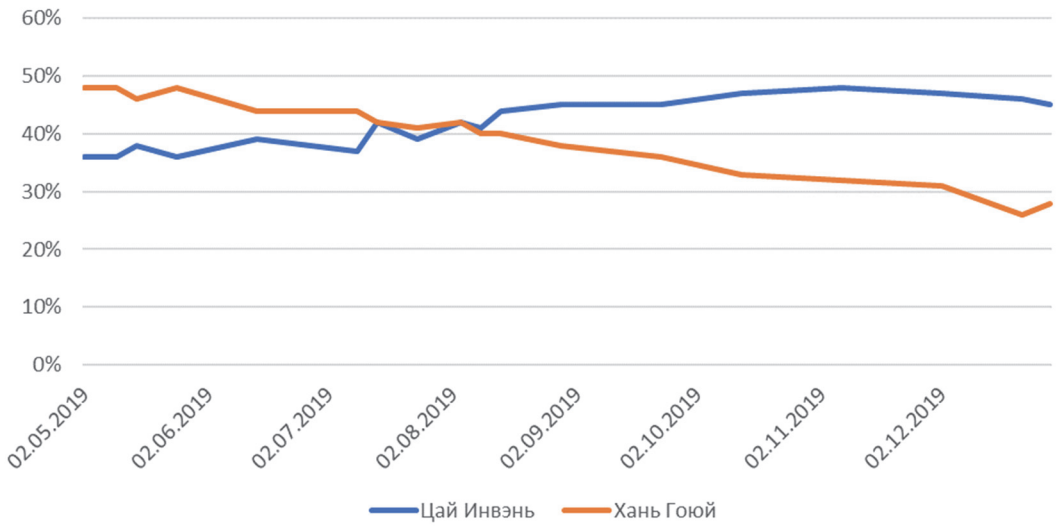

Рис. 1. Рейтинг Цай Инвэнь и Хань Гоюй во время предвыборной кампании на Тайване в 2019 г.
Источник: https://www.datawrapper.de/_/3piBg/
Fig. 1. Tsai Ing-wen's and Han Guoyu's rating during the election campaign in Taiwan in 2019.
Sourse: https://www.datawrapper.de/_/3piBg/

Таким образом, информационная война позволяет Китаю в относительно короткий период времени привести в готовность военные и информационные системы в боевую готовность. По мнению американских специалистов, несмотря на свою эффективность и привлекательность, информационная война может привести и к серьезной дестабилизации и эскалации в наихудших случаях [8. С. 77]. Деятельность США на Тайване провоцирует Китай на начало боевых действий, а с применением информационных методов войны контролировать удары и атаки становится крайне трудным

процессом. Нередко планы по проведению быстрой войны оборачиваются продолжительными конфликтами. Поэтому ведение информационной войны является очень опасным шагом, особенно в конфликте с США за Тайвань. При этом американские ученые уверены, что в условиях неспособности управления информационными атаками Пекин может столкнуться с полным провалом своих политических целей и задач. Зависимость Китая от информационно войны может привести к множеству незапланированных последствий. По мнению специалистов, победу в информационной войне можно одержать, если имеется наступательное преимущество в операциях, существует большая уязвимость объектов для совершения кибератак, а также минимальная возможность эскалации конфликта [30. С. 193, 202, 211]. Только рациональными методами можно добиться наступательного преимущества информационной войны. Использование Китаем информационных атак напрямую зависит от оценок Пекина состояния внешней безопасности и внутренней политики государства.

Заключение

Таким образом, Китай продолжает развивать стратегический курс, направленный на использование информационной войны для достижения своих национальных политических и экономических целей. Пекин поступательно разрабатывает концепции ведения информационной войны, чтобы привлекать к себе чрезмерного внимания со стороны мирового сообщества, уже окрестившее его «Кибер Драконом». Китайское руководство неохотно раскрывают свои стратегические возможности, находится в состоянии постоянной бдительности – это единственный способ избежать неприятных ситуаций. Поэтому чрезмерный интерес КНР к методам ведения информационной войны могут поставить перед мировым сообществом, в первую очередь перед США, сложную и непредсказуемую задачу по обеспечению национальной безопасности.

Библиографический список

1. *Buzan B.* The Logic and Contradictions of Peaceful Rise / Development as China's Grand Strategy // The Chinese Journal of International Politics. 2014. № 7 (4). P. 381–420.
2. *Theohary C.A.* Information Warfare: Issues for Congress. Washington, DC: Congressional Research Service, 2018.
3. *Сунь-Цзы*. Искусство войны. Основы китайской военной стратегии / пер. с англ. СПб: Диля, 2006.
4. *Paterson T.*, *Hanley L.* Political warfare in the digital age: cyber subversion, information operations and 'deep fakes' // Australian Journal of International Affairs. 2020. Vol. 74. № 4. P. 439–454.
5. *Adams J.* Virtual Defense // Foreign Affairs. 2001. Vol. 80. № 3. P. 98–112.
6. *Мигунов А.Л.* Тенденции китайской стратегии ведения информационной войны // Военная мысль. 2008. № 11. С. 62–67.

7. Military and Security Developments Involving the People's Republic of China // Annual Report to Congress. Washington, DC: Office of the Secretary of Defense, 2019.
8. *Евдокимов Е.В.* Политика Китая в глобальном информационном пространстве // Международные процессы. 2011. Т. 9. № 1 (25). С. 74–83.
9. *Krekel B.* Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. Washington, DC: Northrop Grumman Corporation, 2009.
10. Cyberpower and National Security // American Foreign Policy Interests. 2013. № 35 (1). P. 45–58.
11. *Inkster N.* Chinese Intelligence in the Cyber Age // Survival: Global Politics and Strategy. 2013. Vol. 55. № 1. P. 45–66.
12. *Ford C.A.* The Evolution of International Security Capacity Building. U.S. Department of State. 20.11.2020. URL: https://www.state.gov/the-evolution-of-international-security-capacity-building/ [Accessed: 28.12.2020].
13. *Tai Ming Cheung.* The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities // Journal of Cyber Policy. 2018. Vol. 3. № 3. P. 306–326. https://doi.org/10.1080/23738871.2018.1556720
14. Military and Security Developments Involving the People's Republic of China 2013 // Annual Report to Congress. Washington, DC: Office of the Secretary of Defense, 2013.
15. Chuck Hagel. Speech At The Shangri-La Dialogue, June 1, 2013. USC US-China Institute. 01.06.2013. URL: https://china.usc.edu/chuck-hagel-%E2%80%9Cspeech-shangri-la-dialogue%E2%80%9D-june-1-2013 [Accessed: 28.12.2020].
16. *Béraud-Sudreau L.* Assessing Chinese defence spending: proposals for new methodologies. International Institute for Strategic Studies (IISS). 31.03.2020. URL: https://www.iiss.org/blogs/research-paper/2020/03/assessing-chinese-defence-spending [Accessed: 28.12.2020].
17. *Попов И.М.* Война будущего: взгляд из-за океана: Военные теории и концепции современных США. М.: Транзиткнига, АСТ, Астрель, 2004. 443 с.
18. *Панарин* И.Н. Информационная война, PR и мировая политика. М.: Горячая линия-Телеком, 2006. 351 с.
19. *Кошурникова Н.А.* Особенности информационной политики современного Китая // Китай: история и современность: материалы IX международной научно-практической конференции. Екатеринбург, 21–23 октября 2015 г. Екатеринбург: Издательство Уральского университета, 2016. С. 279–284.
20. *Панарин И.Н.* Технология информационной войны. М.: КСП+, 2003. 319 с.
21. *Димлевич Н.* Информационные войны в киберпространстве – Китай и Индия // Международная жизнь. 03.02.2011. URL: https://interaffairs.ru/news/show/614 (дата обращения: 28.12.2020).
22. *Kennedy A.B.* Can the Weak Defeat the Strong? Mao's Evolving Approach to Asymmetric Warfare in Yan'an // The China Quarterly. 2008. № 196. P. 884–899.
23. *Старкин С.В.* Влияние геополитической среды на трансформацию контрразведывательной парадигмы спецслужб США // Вестник Брянского государственного университета. 2011. № 2. С. 130–134.
24. *Wang Baocun*, *Li Fei.* Information Warfare. Federation of American Scientists. 20.06.1995. URL: https://fas.org/irp/world/china/docs/iw_wang.htm [Accessed: 28.12.2020].
25. *Lotrionte C.* Countering State-Sponsored Cyber Economic Espionage Under International Law // North Carolina International Law and Commercial Regulation. 2014. Vol. 40. № 2. P. 443–541.
26. *Joske A.* Picking Flowers Making Honey. The Chinese military's collaboration with foreign universities. The Australian Strategic Policy Institute. 30.10.2018. URL: https://www.aspi.org.au/report/picking-flowers-making-honey [Accessed: 28.12.2020].

27. *Iasiello E.* China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities // Journal of Strategic Security. 2016. Vol. 9. № 2. P. 45–69.
28. Taiwan 2020 Polls. Datawrapper. 2020. URL: https://www.datawrapper.de/_/3piBg/ [Accessed: 28.12.2020].
29. *Kurlantzick J.* How China Is Interfering in Taiwan's Election. Council on Foreign Relations. 07.11.2019. URL: https://www.cfr.org/in-brief/how-china-interfering-taiwans-election [Accessed: 28.12.2020].
30. *Nichiporuk B.* U.S. military opportunities: information-warfare concepts of operation // Strategic appraisal: the changing role of information in warfare. Santa Monica: RAND Corporation, 1999. P. 179–215.

References

1. Buzan B. The Logic and Contradictions of Peaceful Rise . Development as China's Grand Strategy. *The Chinese Journal of International Politics.* 2014;4(7):381–420.
2. Theohary CA. *Information Warfare: Issues for Congress.* Washington, DC: Congressional Research Service, 2018.
3. Sun Tzu. The Art of War: Chinese Military Strategy. Translated from English. SPb: Dilya publ., 2006. (In Russ.).
4. Paterson T., Hanley L. Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'. *Australian Journal of International Affairs*. 2020;74(4):439–454.
5. Adams J. Virtual Defense. *Foreign Affairs.* 2001;80(3):98–112.
6. Migunov AL. Tendentsii kitayskoy strategii vedeniya informatsionnoy voyny [Trends in Chinese Information Warfare Strategy]. *Voyennaya mysl'.* 2008;(11):62–67. (In Russ.).
7. Military and Security Developments Involving the People's Republic of China. Annual Report to Congress. Washington, DC: Office of the Secretary of Defense, 2019.
8. Yevdokimov YV. Politika Kitaya v global'nom informatsionnom prostranstve [China's policy in the global information space]. *Mezhdunarodnyye protsessy*. 2011;9.1(25):74–83. (In Russ.).
9. Krekel B. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* Washington, DC: Northrop Grumman Corporation, 2009.
10. Cyberpower and National Security. *American Foreign Policy Interests*. 2013;35(1):45–58.
11. Inkster N. Chinese Intelligence in the Cyber Age. *Survival: Global Politics and Strategy*. 2013;55(1):45–66.
12. Ford CA. *The Evolution of International Security Capacity Building. U.S. Department of State.* 20.11.2020. Available from: https://www.state.gov/the-evolution-of-international-security-capacitybuilding/ [Accessed: 28.12.2020].
13. Tai Ming Cheung. The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities. *Journal of Cyber Policy.* 2018;3(3):306–326. https://doi.org/10.1080/23738871.2018.1556720
14. Military and Security Developments Involving the People's Republic of China 2013. *Annual Report to Congress.* Washington, DC: Office of the Secretary of Defense, 2013.
15. Chuck Hagel. *Speech At The Shangri-La Dialogue*, June 1, 2013. USC US-China Institute. 01.06.2013. Available from: https://china.usc.edu/chuck-hagel-%E2%80%9Cspeech-shangri-ladialogue%E2%80%9D-june-1-2013 [Accessed: 28.12.2020].
16. Béraud-Sudreau L. *Assessing Chinese defence spending: proposals for new methodologies. International Institute for Strategic Studies* (IISS). 31.03.2020. Available from: https://www.iiss.org/blogs/research-paper/2020/03/assessing-chinese-defence-spending [Accessed: 28.12.2020].
17. Popov IM. *Voyna budushchego: vzglyad iz-za okeana: Voyennyye teorii i kontseptsii sovremennykh SSHA* [War of the Future: A View from Overseas: Military Theories and Concepts of the Modern United States]. Moscow: Tranzitkniga, AST, Astrel', 2004. 443 p. (In Russ.).

18. Panarin IN. *Informatsionnaya voyna*, *PR i mirovaya politika* [Information warfare, PR and the world politics]. Moscow: Goryachaya liniya Telekom, 2006. 351 p. (In Russ.).
19. Koshurnikova NA. Osobennosti informatsionnoy politiki sovremennogo Kitaya [Features of the information policy of modern China] .Kitay: istoriya i sovremennost': materialy IX mezhdunarodnoy nauchno-prakticheskoy konferentsii. Yekaterinburg, 21–23 oktyabrya 2015 g. Yekaterinburg: Izdatel'stvo Ural'skogo universiteta, 2016. P. 279–284. (In Russ.).
20. Panarin IN. *Tekhnologiya informatsionnoy voyny* [Information war technology]. Moscow: KSP+, 2003. 319 p. (In Russ.).
21. Dimlevich N. Informatsionnyye voyny v kiberprostranstve – Kitay i Indiya [Information Wars in Cyberspace – China and India]. *Mezhdunarodnaya zhizn'.* 03.02.2011. Available from: https://interaffairs.ru/news/show/614 [Accessed: 28.12.2020]. (In Russ.).
22. Kennedy AB. Can the Weak Defeat the Strong? Mao's Evolving Approach to Asymmetric Warfare in Yan'an. *The China Quarterly*. 2008;(196):884–899.
23. Starkin SV. Vliyaniye geopoliticheskoy sredy na transformatsiyu kontrrazvedyvatel'noy paradigmy spetssluzhb SSHA [The influence of the geopolitical environment on the transformation of the counterintelligence paradigm of the US intelligence services]. *Vestnik Bryanskogo gosudarstvennogo universiteta.* 2011;(2):130–134.
24. Wang Baocun, Li Fei. *Information Warfare. Federation of American Scientists*. 20.06.1995. Available from: https://fas.org/irp/world/china/docs/iw_wang.htm [Accessed: 28.12.2020].
25. Lotrionte C. Countering State-Sponsored Cyber Economic Espionage Under International Law. *North Carolina International Law and Commercial Regulation*. 2014;40(2):443–541.
26. Joske A. *Picking Flowers Making Honey. The Chinese military's collaboration with foreign universities. The Australian Strategic Policy Institute.* 30.10.2018. Available from: https://www.aspi.org.au/report/picking-flowers-making-honey [Accessed: 28.12.2020].
27. Iasiello E. China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities. *Journal of Strategic Security*. 2016;9(2):45–69.
28. Taiwan 2020 Polls. Datawrapper. 2020. Available from: https://www.datawrapper.de/_/3piBg/ [Accessed: 28.12.2020].
29. Kurlantzick J. *How China Is Interfering in Taiwan's Election*. Council on Foreign Relations. 07.11.2019. Available from: https://www.cfr.org/in-brief/how-china-interfering-taiwans-election [Accessed: 28.12.2020].
30. Nichiporuk B. U.S. military opportunities: information-warfare concepts of operation. *Strategic appraisal: the changing role of information in warfare.* Santa Monica: RAND Corporation, 1999. P. 179–215.

Информация об авторах:
Каткова Евгения Юрьевна – кандидат исторических наук, старший преподаватель кафедры теории и истории международных отношений, Российский университет дружбы народов, e-mail: katkova-eyu@rudn.ru

Юнюшкина Анна Сергеевна – магистрант кафедры теории и истории международных отношений, Российский университет дружбы народов, e-mail: an.yuniushkina2014@yandex.ru

Information about the authors:
Katkova Evgeniya Yuryevna – candidate of sciences (history), senior lecturer, Department of theory and history of international relations, Peoples' Friendship University of Russia (RUDN University), e-mail: katkova-eyu@rudn.ru

Yunyushkina Anna Sergeevna – Master's student, Department of theory and history of international relations, Peoples' Friendship University of Russia (RUDN University), e-mail: an.yuniushkina2014@yandex.ru