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

Research article / Научная статья

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

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: *Katkova E.Yu., Yunyushkina A.S.* Chinese Strategies and Opportunities in Information Warfare: China–US Rivalry in Cyberspace // 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

Introduction

In recent years, the People's Republic of China has shown great interest in information warfare techniques. At the heart of the Chinese postulates on its conduct are the favorable conditions for "restoring its rightful place as the leading power in Asia" [1. P. 387], as well as the further survival and prosperity of its people. Information warfare is not a new phenomenon and has been practiced since antiquity, including by such great commanders as Xerxes and Alexander the Great [2. P. 8]. Military scientists attribute its origin to the writings of the Chinese strategist Sun Tzu, who lived in the 5th century BC. Since ancient times in China there has been a sphere of information confrontation, which gave rise to a special philosophy. It is based on a misinformation impact on the world around, as well as a peculiar style of human thinking. Most of the provisions of this philosophy were presented in the teachings of the military theorist Sun Tzu, whose works are constantly translated into foreign languages [3. P. 38]. The use of disinformation in the conduct of hostilities for Ancient China was very relevant, so the work of this strategist was an important source of useful information. At present, the works of the ancient Chinese strategist continue to be the sources of great interest, are actively used as teaching aids for training personnel of special services, government and other organizations whose field of activity is closely related to cybersecurity. The spread of new technologies and the Internet has allowed countries to practice modern forms of information warfare against each other in innovative ways [4. P. 444].

Today it is known that many countries, including democratic ones, use information to achieve strategic goals.

Both democracies and autocracies seek to develop their cyber technologies in order to gain an advantage in defensive and offensive capabilities. In this area, however, autocracies are in a better position. First, in democratic countries, civil society requires transparency in decision-making and budgeting, which significantly limits military circles in financial matters. Secondly, the defensive technologies of democracies are also less developed, in particular, disinformation easily penetrates the national segments of the Internet due to freedom of speech, which makes it very difficult to find and block malicious messages or fake news that penetrate through advertising and social networks. While autocracies have either already developed mechanisms to regulate the Internet, in particular the Chinese "Golden Shield" (金盾工程), or seek control by improving national legislation in this area. Thus, China has a comparative advantage over the US and other Western countries in defensive and offensive information warfare technologies.

The brilliant achievements of the United States in the development of information technology at the end of the 20th century led China to pursue a political course aimed at developing strategies for waging information warfare.

In the past decades, China has undergone military modernization, which caused concern among the international community, as China concentrated on the development of network forces, namely: it launched a program to conduct developments in the field of information warfare tactics, which involve the presence of special units and specially trained personnel with the necessary knowledge and skills in the field of information technology and advanced systems [5. P. 100]. As a rule, the training of such specialists takes place in state academies, universities and special educational institutions. The Chinese leadership pays great attention to the issue of involving young professionals in the field of information technology. The increasing number of Internet users in China every year makes it possible to identify the most active and advanced amateurs. In addition, unlike democratic countries Beijing can use significant resources and spend huge amounts of money on the development of modern doctrines of information warfare to maintain the defense capability of its country [6. P. 63]. The rapid development of military technologies turns China into one of the global leaders in information warfare [3. P. 40, 68, 73]. China considers information as the central instrument of state and military power [7. P. 56]. Thanks to the huge success in the development and implementation of information technology, the rapid changes in nuclear weapons, ballistic missiles and space innovations, the People's Republic of China has all the chances to come to the fore in the near future in information warfare programs.

The rivalry between China and the United States in the information sphere

In 1997 and 1999 the US military experienced the first attacks of Chinese hackers, which made the US government think about the real threat to national security from China [8. P. 81]. A series of attacks on US civilian and military bases were unexpected for The United States Central Command, causing concern in the highest political circles. Today, China is using information attacks for security purposes in Southeast Asia, a region that also occupies an important place in US foreign policy. Information security began to play an important role due to the recent events in the region, in particular after the start of the rivalry between China and the United States for influence in Asia.

Since the beginning of the XXI century some major US government systems have been subjected to major cyberattacks by China. According to a number of American experts, these attacks were carefully prepared and developed through the information received from the intelligence services. The targets of these attacks were the Internet networks of the infrastructure objects to search for weaknesses and vulnerabilities [9. P. 12]. To be effective in cyber-attacks on US defense and industrial establishments, Beijing has resorted to the use of technical equipment under the direct control of the Chinese People's Liberation Army (PLA). Washington believes that the Chinese leadership will continue to carry out operations to obtain not only data of a defense and scientific and technical nature, but it will also concentrate on the collection of political and economic intelligence information concerning commercial and non-governmental organizations, which is under the jurisdiction of the Ministry of State Security of the PRC [9. P. 7]. Additionally, it should be noted the wide scale of cyber espionage by China, which is aimed at the public and private sectors of the United States. For example, the American AMSC company was subjected to a cyber-attack by China aimed at obtaining software for further use in the state-owned enterprise Sinovel, which significantly affected the income side of the American company [10. P. 48]. Canadian telecommunications company Nortel has also been subjected to industrial cyber espionage by China [11. P. 50]. The rapid pace of China's economic development allows Beijing to increase the effectiveness of industrial espionage against Western countries.

Since 2010s the rivalry between China and the United States in the information space continues to increase, which may lead to a more "hot" conflict that will affect the current international situation. In 2010, the United States accused China of hacking into the email accounts of human rights activists, which led in 2013 to harsh recriminations from officials of the two states. In March 2013, US President Barack Obama issued a special executive order regarding government procurement procedures for high-tech solutions. Under this order, the U.S. Department of State prohibited cooperation with China in the procurement of IT equipment for public sector organizations [12]. This order also caused discontent both inside the United States and abroad. As a result, IT giants such as Apple, Dell, HP, etc., which are directly dependent on China's production capacities, suffered significant losses. The Chinese leadership protested against such similar actions by the US President, since the suspicions raised against Chinese companies have no basis, which means that this policy is more reminiscent of non-market methods of protectionism [13. P. 312].

In the spring of 2013, the US Department of Defense delivered a report to Congress titled "Military and Security Developments Involving the People's Republic of China 2013" accusing the Chinese government and the PLA of carrying out hostile cyberattacks on the US Department of Defense and other key American institutions. "China is using its computer network exploitation capability to support intelligence information collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs" [14. P. 36]. The American establishment believes that China is trying to establish control over the Internet space in order to expand its "digital sovereignty". In May 2013, the then US Secretary of Defense Charles Heigl, on the sidelines of the Asian Security Summit in Singapore, said that the number of cyber attacks by China made against military and government facilities is constantly increasing [15]. In response to this statement, the director of the Center on China-American Defense Relations, established under the Academy of Military Sciences of the PLA, retired major general Yao Yunzhu said that Washington is constantly increasing its military presence in the Asia-Pacific region, thereby calling into question the trust in Sino-American relations [16].

Thus, it becomes clear that China and the United States openly recognize the issues of information warfare and classical forms of military presence, which play an important role in the system of regional and global security. Every year, the PRC improves and develops the strategy of conducting a network information war, which has a direct impact on the policy of the United States [5. P. 110].

China's Information Warfare Concepts

The concept of "Information Warfare" arose in the mid-1990s of 20th century in the United States' academia and scientific circles as an object to ensure the intellectual security of the state. Gradually, the "intellectual fever" swept over the political leadership of China. As a result, extensive developments have begun to ensure information security [17. P. 440]. Beijing believes that information and information security is essential to the survival of the Communist Party of China (CPC), and dominance in this area can help ensure this. No one could have expected such a rapid rise in this area in China, since there was not a single published statement from Beijing, which at that time was actively engaged in secret developments to maintain national security. Thus, we can talk about China's growing interest in the tactics and tools of the information war and the triumphant end of the information revolution [17. P. 426].

The Chinese concept of network warfare opens up further prospects and opportunities for the Chinese leadership and military specialists to work on the creation and implementation of the latest technologies. China from time to time organizes meetings to discuss methods of information warfare [18. P. 312], and the PRC military experts are developing the necessary theoretical concepts for its successful implementation [19. P. 280].

At present, the PRC has embarked on the path of seeking information superiority. The Chinese are developing opportunities to use information warfare technologies to achieve their political goals. This is not a direct threat to US national security but puts Washington in a vulnerable position [19. P. 281].

The main consequences of the information revolution in China include: firstly, Beijing recognizes the importance of high-tech innovation and new information technologies; secondly, Beijing intends to become a major political and economic power, as well as firmly strengthen its position in the international arena. It should be noted that the Chinese leaders attach great importance to the economic development of the country, which is the highest national and state priority in the information and economic sphere; thirdly, Chinese experts believe that thanks to the constantly growing national power, China will continue to maintain a leading position among the leading players in the multipolar world; finally, the ability to successfully compete economically and wage high-tech warfare will become the main national components of China's strength and power [6. P. 65].

It is worth noting that information wars contribute to compensating for the quality and quantity of military technologies in China, since the methods of conducting information warfare allow the Chinese leaders to wage a distant and secret war with the strongest military powers, such as the United States and European countries [20. P. 300]. Information warfare in China is based on non-standard methods and capabilities that make it possible to avoid assaults and attacks from the enemy. China is in a constant process of developing tactics aimed at deterrence and securing victory against the strongest powers. According to some experts, Beijing has great potential to achieve superiority over the United States in the information sphere [21]. China has the ability to attack very vulnerable US infrastructure facilities or influence domestic political processes, thereby weakening and undermining US position in the international arena. Mao Zedong's thoughts on waging war, using weaknesses to achieve victory over a strong enemy, still have a significant influence on the minds of the top Chinese military [22. P. 899]. Chinese experts also believe that the information warfare is a kind of arena in which supremacy among world powers is determined. The Chinese government believes that the information warfare contributes to the rapid build-up of the military power of the Celestial Empire [18. P. 313].

China considers military superiority over the United States as the main guideline for overcoming and solving all problems in information and military terms. China is confident that new information technologies will significantly increase the capacity of existing equipment at no significant cost. For example, information gathering means such as satellites and related intelligence systems require significant financial investment, therefore, over the past two decades, Beijing has been pursuing a rational economic policy for the stable development of information technology.

The approach of the Chinese leadership to the definition of information security diverges significantly from the Western understanding of the meaning of cybersecurity. For example, the Western approach significantly contradicts the Chinese one in terms of the degree of openness of the global network – the Internet [23. P. 130]. Tight control of the Internet in China is aimed at blocking the further dissemination of unwanted information within the state, as well as preventing the leak of secret information outside the country. By restricting access to the main social and search systems, the PRC leadership also controls the flow of information and exchange between users of the global network. In the US, the term "cybersecurity" refers primarily to the security of the systems of the Internet. In the PRC, this term means "information security" (信息安全), which is aimed at combating the spread of unwanted information. The presence of a significant difference in approaches to the definition of the term between the two states greatly complicates the conduct of negotiations between them [8. P. 72].

Chinese analysts place great hopes on information warfare and divide it into two categories, namely, the development of offensive and defensive information warfare capabilities [19. P. 283]. The main methods of conducting offensive operations include direct attacks on enemy information systems, which paralyze and weaken the enemy command and control system [24]. In addition, espionage is an important tool too. Now it has become a favorite method of collecting information by both state and non-state actors, in particular intelligence agencies [25. P. 445]. This is evidenced by numerous cases of the theft and transfer of American intellectual property to China to promote technological developments in both the civilian and military spheres [26]. In 2012 alone, the United States estimated losses of approximately $338 billion as a result of cyber espionage [27. P. 45].

Every year China pays more and more attention to developing potential strategies for successful information warfare. The essence of these strategies is to increase resistance to interference, strengthening protection against all kinds of attacks. Protecting its own information platforms and ensuring the normal functioning of systems are becoming equally important components of China's defense policy [21].

The Chinese leaders believe that the use of offensive and defensive operations in the course of information warfare requires a proven and effective command and control system [8. P. 78]. The end result of the information war directly depends on command and control, which affect most information operations and regulate the overall situation. Any mistake made puts the entire information system at risk. Therefore, the issue of coordinated command and control requires increased attention [24]. One of the main components of success in the information war is to obtain timely information about the real situation in the enemy's country to ensure self-security [6. P. 64]. At the first stages of information warfare, it is necessary to deprive the enemy of the ability to acquire, process and transmit data, while ensuring the protection of their own information systems. For example, a complex of control systems is aimed at ensuring the accuracy of strikes, at conducting electronic warfare to disable attacking enemy systems [6. P. 65]. To maintain effective command and control, it is necessary to apply a wide range of information technologies that are highly reliable in remote sensing and reconnaissance. Obviously, high-resolution photographs obtained from satellite surveillance systems, infrared detection systems, unmanned reconnaissance aircraft, etc. will be further used and developed [17. P. 37, 98, 201]. Thus, the main tools of offensive and defensive information warfare in China include: physical destruction; cyber espionage; dominance of the electromagnetic spectrum; computer network war; psychological manipulation [19. P. 284].

It is also worth highlighting the main aspects of information warfare. The Chinese government emphasizes the importance of, first of all, the accuracy of striking the enemy [18. P. 284]. Stealth weapons will be able to perform precise strikes, which are carried out using sound and electrical waves, visible light and infrared rays. Chinese analysts agree that competition for the electromagnetic spectrum will be the most important stage in the information war, and its goal will be to dominate the enemy in the use of electronic equipment [18. P. 110, 201, 286]. Gradually, microelectronics will become a key technology area for investment. Chinese experts state that a network of computer wars is taking on more and more diverse forms, which can manifest themselves both in cyberattacks and in hacker wars. Analysts view virtual warfare as an instrument of false commands to deceive enemy forces [8. P. 82]. The Chinese military is actively showing itself in virtual simulations of real combat operations.

Another widespread method of information warfare is psychological warfare, which involves the spread of disinformation to have a devastating effect on the emotional and physical health of people, which leads to a noticeable weakening of the enemy. In the course of psychological warfare, tools such as media propaganda are used; distribution of paper leaflets; sending spam information to email addresses and social networks. There are technology developments in the field of remote sensing and exploration in China [19. P. 284]. Work is underway to introduce photoelectronic technologies that will be widely used in the future. These technologies include taking sharper photographs; increasing the speed for information transfer; the presence of compact and small-sized dimensions of the equipment of photoelectronic systems.

China is also actively developing the space industry, increasing production capacity for the effective detection of enemy forces [20. P. 300]. The military personnel of the PLA participate in joint work with leading experts in the field of military mapping, remote sensing and satellite navigation [21].

Based on China's interest in information warfare, we can say that the PRC is allocating significant funds for the creation and acquisition of modern information technologies in order to create a powerful information military force. China's active advancement in the space industry will create a modern and efficient intelligence system that will become a significant component of the Chinese military forces. Moreover, in addition to new technologies, the information war will support the policy and strategies of the PRC [8. P. 80]. China seeks to achieve its political goals by peaceful means, excluding a real armed clash. In many of China's activities, information warfare methods are conflict prevention tools by striking at the enemy's vital points, namely the command and control of information systems. According to some American experts, China's "obsession" with information technology poses the most dangerous and unpredictable challenge to US security [21]. If we take into account the conflicts in Taiwan, we can see that Beijing used information warfare methods to delay the deployment of US military forces in Taiwan. The American troops, although possessing high-tech equipment, could not prevent PC hacks and the weakening of information systems. Thus, the arrival of American warships to the shores of Taiwan was delayed, and the PRC began a large-scale deployment of a complex of short-range ballistic missiles in the direction of the accumulation of American military structures [24].

China has also used all kinds of information warfare during the 2019–2020 Taiwanese presidential campaign and presidential elections. In particular, hackers and bots spread misinformation through social networks such as Facebook, microblogging Weibo services, and popular chat apps such as Line. The PRC has also stepped up propaganda through Taiwanese media bought by Chinese tycoons [29]. It is worth noting the effectiveness of such actions. According to various public opinion polls, the pro-Chinese candidate Han Guoyu, a representative of the Chinese Nationalist Party, was in the lead in the ratings for quite a long time, but the events in Hong Kong confused the cards allowing the representative of the Democratic Progressive Party, Tsai Ing-wen to win (Fig. 1).

Thus, information warfare allows China to put its military and information systems on alert in a relatively short period of time. According to American experts, despite its effectiveness and attractiveness, information warfare can lead to serious destabilization and escalation in the worst cases [8. P. 77]. US activity in Taiwan provokes China to start hostilities, and it becomes extremely difficult to control strikes and attacks with the use of information warfare. Often, plans for a quick war turn into long-term conflicts. Therefore, conducting an information war is a very dangerous step, especially in a conflict with the United States over Taiwan. At the same time, American scientists are sure that in the conditions of inability to control information attacks, Beijing may face a complete failure of its political goals and objectives. China's reliance on information warfare could lead to many unintended consequences. According to experts, it is possible to win an information war if there is an offensive advantage in operations, a greater vulnerability of objects to cyber attacks, as well as a minimal possibility of conflict escalation [30. P. 193, 202, 211]. Only rational methods can achieve the offensive advantage of information warfare. The use of information attacks by China directly depends on Beijing's assessment of the state of external security and domestic policy of the state.

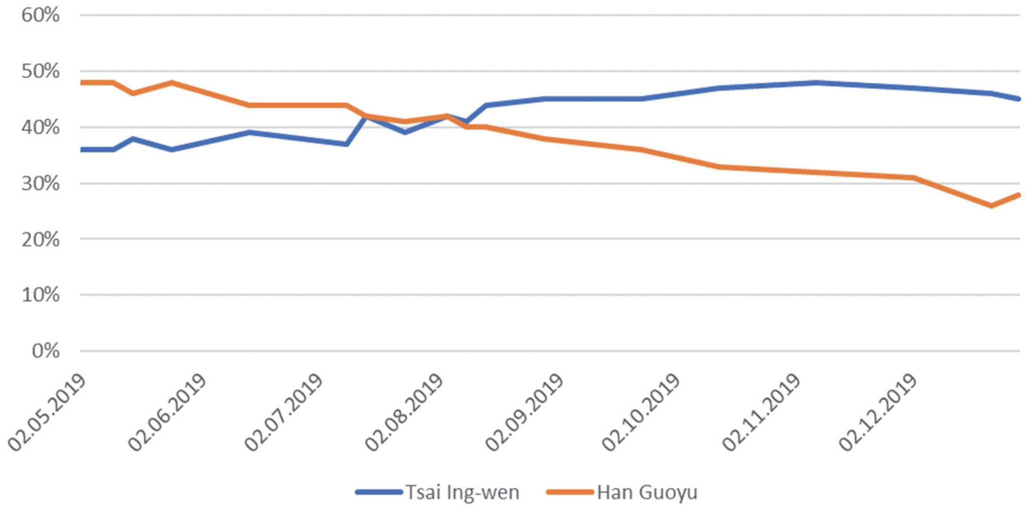

Fig. 1. Tsai Ing-wen's and Han Guoyu's rating during the election campaign in Taiwan in 2019.
Sourse: https://www.datawrapper.de/_/3piBg/

Conclusion

Thus, China continues to develop the strategic course aimed at using information warfare to achieve its national political and economic goals. Beijing is progressively developing the concept of introducing the information warfare in order to attract excessive attention from the world community, which has already named it the "Cyber Dragon". Chinese leaders are reluctant to reveal their strategic options and are in a state of constant vigilance, as this is the only way to avoid unpleasant situations. Therefore, China's excessive interest in information warfare methods can set a difficult and unpredictable task to the world community, primarily the United States, to ensure national security.

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.

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.

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

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