UDC 004.056.5

I.S. Vasilyeva

USA, China and Essential Focus on Strategic Cyberwarfare

The current dependence of the information and cyber component has made our civilization much more vulnerable. The speed and wide dissemination of information technologies and networks have caused a tremendous increase in information and cybernetic arms power. With the growing role of cyberwarfare in the international politics, leadership in cyber sphere is one of the main ways to achieve national strategies. Being geopolitical opponents in reaching superiority in world cyberspace – USA and China are the key leaders in charge of cyberwarfare. In the paper the definition, initial priorities of cyberwarfare, along with development of the cyber strategies of USA and China, their balance of power and future coexistence are revealed.

Keywords: cyberwarfare, security, USA, China, national strategies, cyber command, information warfare.
doi: 10.21293/1818-0442-2017-20-3-161-166

Introduction – What Is Cyberwarfare?

The rapid development of informatization worldwide, specifically in the USA and China, and its penetration into all spheres of the vital interests of an individual, society and state, has undoubtedly brought not only advantages, but also led to the emergence of a number of significant problems. The urgent necessity of protecting information along with being protected from it has become one of them. When economic wars due to the integration of national economies become too dangerous and unprofitable, global military conflict is capable of leading to the extinction of all life on the planet. The war acquires new directions and qualities: information warfare with a great thirst for comfort in it and cyberwarfare. Today information resources have become the wealth of a country, like its minerals, production and human resources. Considering that economic potential is increasingly defined by the level of development of the cyber structure, the potential vulnerability of the economy to information and cyber influences grows in proportion.

The amount of cyberwarfare financing demonstrates that leadership in this sphere is considered one of the main ways to achieve national strategies. Cyberwarfare is not some hazy futurology sector but a real «discipline» which is being studied and developed, gaining more and more secretive, deeper forms. There is no official definition of cyberwarfare yet, thus the one created by RAND Corporation will be used: «cyberwarfare involves the actions (offensive or defensive) by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks» [1]. In addition, the United States Department of Defense (DoD) defines cyberwarfare as «an armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyberattack, cyber defense, and cyber enabling actions». [2].

Achieving success in any war, above all in the cyber one, is impossible without the availability of reliable information and intelligence. For these purposes, foreign intelligence services use a variety of techniques and methods, from monitoring the mass media to the most sophisticated ones, including industrial espionage and technical reconnaissance. The bet is on «smart» weapons guided by satellites, microwave bombs and drones [3]. According to Barack Obama, «it's now clear that this cyber threat is one of the most serious economic and national security challenges we face».

In the arena of information/cyber confrontation, we now see not just national states but also blocks of countries united by common international political interests. Thus, the necessary resources (material, technical, human, intellectual) can be in completely different parts of the world, but work perfectly as one single organism for providing information and cyberwarfare. The role of cyberwarfare in international politics is growing every year. The image aspect is especially significant. Cyber, information and psychological factors will be the most important in world politics. However, cyberwarfare affects not only the mass consciousness, but also the decision-making process of the world's political elite. Therefore, the results of cyber confrontation have real financial, economic and geopolitical consequences for states.

Advances in technology, ongoing geopolitical transformation, and an increasing number of economic and social developments can radically alter the realities of today. The range of possible scenarios is wide and difficult (or impossible) to predict. In such circumstances, the central problem is, therefore, the development of the direction that will effectively respond to any scenario. It determines the need for constant adaptation of forces to the tendency.

Who Is In Charge Of Cyberwarfare?

Today, the strategic geopolitical advantage and economic prosperity of any country is mostly dependent on the degree of its involvement in the cyber sphere. Cyber is an essential basis for making decisions in production, objects of civil and military infrastructures, public authorities and daily life.

In comparison with other countries, the United States (US) has a significant advantage in the field of the development and use of information and telecommunication technologies, and has the highest level of computerization. Based on established practice, the US consolidates the dominant positions not only in the po-

litical, economic and military spheres, but also in the global information/cyber infrastructure. This information/cyber dominance produces an ironic asymmetry. The United States is both powerful and vulnerable.

The main strategic US priority is to be active in cyberspace in order to secure world leadership. After all, it is the US which annually sustains enormous losses from cybercrime and leaks of commercial information. The US openly bets on cyberwarfare techniques to achieve superiority in cyberspace and the conservation of leadership positions in the 21st century. The signals intelligence collection and analysis network «Echelon», «Prizm», «NarusInsight», etc. are the key components and great «helpers». Special counsel and the sixth Director of FBI, Robert Mueller, said that in the near future cyber threats can potentially be equated, and can even surpass the threat posed by terrorism.

The US continues to improve the concept of cyber and information warfare. The main direction is in expanding the applicability of techniques and methods of this warfare. The US divides actors in cyberwarfare into four types: hackers, organized crime groups, terrorist organizations/networks, and advanced state/nation. In early 2013, the US Cyber Command (USCYBERCOM) announced the formation of offensive cyber divisions, the number of which reached 40 in 2015. By the end of 2017, it will be split into more than 60 cyber defensive divisions, which will provide a defensive function. Each team will have a combination of experienced engineers, software (including civilian contractors) and staff with more specific skills. US Cyber Command receives a huge budget from the state, and has contacts all over the world. Most of these teams (40 offensive and 60 defensive) will be assigned to other commands (for example, to the US Navy special forces), but about 13 (according to open-source information) will be used for retaliation in the case of an attack on the US [5–7].

Cyber Command became operational in late 2010, and is still working. Only in 2013, after multiple technical, legal and political issues, they have reached the «authorization to operate» agreement. The year before, the US Congress approved a new law that allows the Ministry of Defense to conduct offensive operations of an information-cybernetic nature, in response to cyberattacks on the US [6–8]. The US military is now allowed to wage war in cyberspace. The new law requires that all the rules that apply to conventional war also apply to cyberwar. This includes the international law of armed conflict (to prevent war crimes and unacceptable behavior in general) and the US resolution on the right of declaration of the war (which requires obtaining the permission of the US Congress within 90 days after entry into the war). Also in 2013, the US Department of Defense announced that nuclear weapons could be used as a response to a cyberattack. However, it should be noted that, for example, the NSA doesn't have all these restrictions because it is an intelligence agency [9].

Meanwhile, there are some problems with finding qualified people to carry out attacks and counterattacks. US Cyber Command has small organizations that coordinate the activities of cyberwarfare among other units, as well as other branches of government and commercial organizations which participate in the network security. However, in most cases the main manpower of Cyber Command deals with the four major US services (Army, Navy, Air Force, Marine Corps).

Out of the four services, the US Air Force is the most experienced in matters of cyberwarfare. Back in 2008, the Air Force planned to formally establish its own Cyber Command, which was to exceed the capacity and ability of the «ordinary» Cyber Command. This new organization of the Air Force was supposed to officially begin it work at the end of 2008. Instead, the main staff was sent to the new nuclear command. This change was made in response to the growing (at the time) problem of the Air Force's nuclear weapons. Despite this, the Air Force continued to try to create a new cyber command and use it to gain full control over the conduct of cyberwarfare. Back then, other services were not so interested in cyberwarfare, which eventually led to the creation of the 24th Air Force, which deals with cyber and electronic warfare. Following the example of the Air Force, the US Army has also created a cyber command. About 21,000 soldiers were withdrawn from the electronic and intelligence units in order to form the US Army Cyber Command (ARCYBER), which was founded in 2010 and became fully operational in 2012. In 2009, the US Navy created the Information Dominance Corps and in 2010 it formed the 10th Fleet of the US Navy with more than 40,000 IT staff. While the usual Cyber Command is focusing on exploration and network security, the Navy Cyber Command also includes data related to meteorology and oceanography. The Navy called up about 45,000 talented sailors and civilians, the majority of whom were reorganized in the 10th Fleet. One thousand new positions were created, mainly for the 10th Fleet. All this has given the Navy a more powerful and secure position in cyberspace. The US Marine Corps also created its Cyber Command in 2010, consisting of approximately 800 employees, which should ensure the safety of the Marine network [10–12].

The participation of the US administration in the development of the area and the security of cyberspace was first noted in the released National Strategy for 2003. Cybersecurity policy in the US continues to develop and has already changed; now the emphasis is not on non-state terrorist actions and state actors (in the framework of the National Security Strategy, 2010). Also, in May 2011, the United States released its International Strategy for Cyberspace, which clarifies and unifies American attitudes towards international partners in matters of cybersecurity [6].

The character of US policy led to the fact that the processes of development of the cyber strategy and action plans have been fragmented. However, currently there is a wide network of national plans that set cyber standards and goals. In April 2015, the DoD Cyber Strategy was updated and published. The original DoD Strategy for Operating in Cyberspace was published in

July 2011. In June 2015, the US Department of Defense included a chapter dedicated to cyberwarfare in the DoD Law of War Manual. Attention to the debate about cyber threats and cyberwarfare continues to grow. Institutions and the administration continue to lobby Congress for regulation and the adoption of a comprehensive cyber security strategy. In April 2015, the US DoD published the latest Cyber Strategy; here are the five pillars of the US military strategy for cyberwarfare [13]:

1. Build and maintain ready forces and capabilities to conduct cyberspace operations.

2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions.

3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber-attacks of significant consequence.

4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.

5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

The new US cyberwarfare strategy that was announced by the Pentagon on April 2015 says, «as a matter of principle, the United States will seek to exhaust all network defense and law enforcement options to mitigate any potential cyber risk to the U.S. homeland or U.S. interests before conducting a cyberspace operation» [13]. But it also adds that «there may be times when the president or the secretary of defense may determine that it would be appropriate for the U.S. military to conduct cyberoperations to disrupt an adversary's military related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyberoperations to terminate an ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests» [13]. So far, most American cyberattacks on enemies have been covert operations, but now the door seems to be open for preventive cyberattacks [14]. The new strategy also explicitly names China, Russia, Iran and North Korea as the countries most likely to pose a cyber threat to the US [13].

On a level with the US, China is another world leader in charge of cyberwarfare. In the coming decades, this nation appears to hold the greatest potential for developing into a real rival to the United States. The strengthening of China, obviously, will lead to a new configuration of geostrategic forces in the world, i.e., a new structure of international relations [5]. The unavoidability of the future geopolitical confrontation with the United States demands that the Chinese leaders be carefully prepared for cyber operations under modern conditions. It should be said that cyber geopolitics is the most restricted in China. They pay a lot of attention to the development of mass media and the Chinese Internet.

China is actively promoting the concept of a Special Forces network (battalion-sized units), which should consist of highly qualified computer experts. Active youth are the most welcomed, especially Internet users. Thus, the main priority is the strategic course on concept development of the effective use of cyberwarfare to achieve main political and economic targets. China is currently executing a patient and deceptive form of cyberwarfare designed to advance its economic state, maintain its national unity, significantly improve its technological and military capabilities, and increase its regional and global influence with minimal or no fighting and without alarming the West, using cyberwarfare based on its strategic heritage to achieve its national interests [15].

The Chinese military already has a cyber army, whose population is growing at an incredible rate. It has created a huge number of academies, colleges and universities with extensive training courses that are aimed at preparing information and cyber units. These units plus voluntary organizations and the Golden Shield (Internet censors and monitors) cooperate closely with each other, providing China with unimaginable opportunities in cyberwarfare [16]. Together, they can conduct a huge attack and have great defensive potential. No other country has anything like that yet.

In the opinion of commanders of the People's Liberation Army of China (PLA), one of the key factors that has a significant impact on conflict resolution is superiority over opponents in cyberspace. If we talk about what the PLA is from the point of view of the organization of the army, it's divided into divisions, each responsible for one thing: electronic warfare, electronic defense, intelligence gathering and cyber operations. Despite the separation of duties, the Chinese military is well-equipped and staffed. The PLA General Staff Department Third Department (Department of Technical Intelligence, Jishu Zhencha Bu) is responsible for technology exploration, as well as data collection and analysis, and provides communication security for the PLA [17–19]. It's often compared to the US NSA. The Fourth Department (Department of Electronic Warfare and Electronic Countermeasures) is responsible for offensive operations in the electronic warfare and countermeasures exercise.

For more than a decade, the PLA has been studying US military publications on the network war (and now cyberwarfare) and doctrines of information warfare. After observing the American information operations in the Balkans and the first Gulf War, the PLA has seen the effect of modern information operations on the battlefield and the international arena. Then, the PLA began to design its own form of information warfare. [17, 20] Over the past 25 years, the Chinese military adopted the concept of information warfare appropriate for its organization and doctrine, mixing its traditional tactics, military approaches of the USSR and the US doctrine for the introduction of the PLA in the information age. At the same time, the PLA modernized to improve its own military and psychological operations and expanded the role of its research centers.

China's military doctrine is dependent on information technology and cyber operations. The operational

concept of the PLA for conventional intelligence and electronic warfare has been extended to cyberwarfare; kinetic and cyberattacks aimed at satellites; and information warfare. Along with these technical aspects of Information Operations, the PLA combines them with psychological and media war operations. Understanding the concepts of new PLA strategy is important for the US and other allied military leaders.

«Cold cyberwar» and balance of power

U.S. military experts have recently come out with official accusations against Beijing, catching them in the creation of tools for organizing cyberattacks and developing viruses as well as supporting special IT-troops, including hackers who occasionally commit diversion activities against other states [21]. This activity is a part of Chinese military foreign policy. In addition, many in the American defense community worry that China's growing presence in the manufacturing sector provides it with plenty of opportunities for mischief which they may not be shy to take advantage of. In fact, the analysis of Chinese-made chips (which were used in many systems, including weapons, nuclear power, public transport, etc.) conducted by American specialists in the IT sphere has shown that they contained malicious code that was placed by the manufacturer and that was able to remove cryptographic protection from main chips as a means of changing the encryption key and getting access to an unencrypted flow of information or to even disable it. In addition, according to the researchers, this kind of beetle can be used as a weapon and as a sort of advanced version of a well-known Stuxnet.

In May 2012, in the annual report of the US Department of Defense on the PLA (in the US Congress), it was pointed out that China's telecommunication companies, such as Huawei, Datang, and Zhongxing (ZTE), have links to the Chinese government and the PLA. Also, General James Cartwright said that China had cyber reconnaissance and mapping of public and private computer networks necessary for carrying out cyberattacks and has the ability to incapacitate critical infrastructure and military control of the US. Chairman of the Joint Committee of the US Joint Chiefs of Staff, General Martin Dempsey, urged China to cooperate with transparency and an exchange of technology.

In 2013, President Obama discussed US concerns about cyber espionage with Vice Premier Wang Yang and Foreign Minister of China Yang Jiechi. US Secretary of Defense Chuck Hagel stressed the necessity of cooperating in cyberspace. In March 2014, Chuck Hagel said that the number of US cyber professionals will be tripled [21]. Frequent attacks on the part of Chinese hackers on the information systems of US companies have even become the subject of a conversation between Barack Obama and Xi Jinping. The damage from Chinese economic espionage is valued at more than $300 billion; some media have already named this «cold cyberwar» [22].

China has a very high scientific potential, qualified and experienced staff, and the modern material resources that are necessary to successfully carry out research in the IT sector. It extensively collaborates with leading academic institutions and research organizations in the field of «critical technologies.» As a result of this interaction, China has access to advanced research, technologies and telecommunication systems that can be used for military and dual purposes. The most remarkable fact that highlights the possibility of Chinese experts hacking well-protected networks is separate opinions about Chinese involvement in the penetration of the Pentagon network, when one of the main computer networks was paralyzed (in the US, this series of cyberattacks is called «Titan rain») [21-23].

China «sees» objective cyber factors that help achieve a balance of power with rival parties. More importantly, a key factor in cyberspace is its invisibility. The demonstration of power in the cyber world is different from forces with tanks. Therefore, comparison with the old boundaries is no longer appropriate. The combination of the objective factors of cyberspace and strategic thinking has allowed China to increase its digital capacity. China launched cyber intelligence and espionage a long ago, and today China's cyber activity [24, 26] aims to develop a strategic advantage.

The US must resist the growing Chinese intelligence. China's cyber strategic advantage can lead to the use of cyber sabotage operations against the major powers. Following are three points of China's strategy, which can be identified as the most problematic for US cybersecurity:

1) China hopes to receive information via cyber reconnaissance of enemy systems, manipulation and influence on the perception of the technology of opponents – in other words, to obtain a cyber strategic advantage.

2) China understands that if the country is in a state of crisis, it can be used as a strategic advantage. Therefore, cyber exclusion and reconnaissance will be included in subversive (sabotage) activities.

3) After the discovery of vulnerabilities, China can make the cyber/information technological systems of any potential enemy useless, and use the resulting benefits to create a full-scale cyber offensive.

According to US research, China now captures terabytes of data from cyber-information systems of foreign nations by sensing intelligence. China has developed ready-to-use offensive cyber and national defense organizations. Defense and attack are key components of cyber strategy. In contrast to this, the US is at a significant disadvantage; the vulnerabilities of US infrastructures have been already documented by the PLA. China is able to contain and potentially win over the US and any other country in cyberspace.

However, despite all the accusations that China is a major source of various online attacks (and not only against the United States), officials declare that they will cooperate with the further development of mechanisms of cyber defense and control over cybercrime. Both countries have greatly moved forward in the progress of technological solutions and a joint fight against cybercrime that will help prevent a global crisis in this area.

Obama and the president of China, Xi Jinping, reached a mutual agreement that both countries won't commit cyberattacks or commit intellectual property theft through the Internet [5]. Earlier, Chinese authorities had angrily reacted to the statement by the US Director of National Intelligence, James R. Clapper, about hacker attacks and asked to stop «unreasonably blam[ing] them for that».

Meanwhile, Chinese hackers still regularly attack US industry, in particular, engaging in cyber espionage. The US Congress expressed a proposal: to allow companies and individuals affected by the hands of Chinese hackers obtain «revenge» for themselves and attack hackers back [6]. The Commission, dealing with issues of economic relations and security between China and the United States, submitted to Congress a report that announced the bold idea. The Commission has traditionally criticized Beijing and reported that the number of cyberattacks on the business sector from China continues to grow, and that companies have had billions of dollars in losses, becoming victims of cyberespionage. In many cases, the stolen secrets from US companies were transferred directly into the hands of companies owned by the Chinese government. One of the most high-profile breakups was the attack on the US Office of Personnel Management; this compromised the personal data of about 22 million people [5, 18, 24-25]. According to the available information, the penetration happened in December 2014, but state IT professionals detected it only in April 2015.

Currently, there is no one to stop China from its cyber conquest; a study of the process of the strategic thinking and paradigms of China can help develop appropriate countermeasures. Another option is the development of alternative networks which are not available for either China or other cyber opponents. Deceptive measures can also be used to expose the participants and partners of cyberwarfare. These and similar actions can undermine the real strategy of the PLA. However, as China continues to increase economic, military and political strength, it is essential that American strategists devote greater study towards understanding the adversary. China, like a chameleon, will adjust to any conditions, so there is a crucial need to stay alert.

Conclusion

Cyberwarfare has become the most important geopolitical factor defining the destinies of countries and civilizations. What awaits us? It is obvious that the future will offer even more problematic scenarios for armed forces around the world. Cyberspace will continue play an important role in future military operations. China is becoming a real rival of the US, and the US should increase economic and political potential to lead a balanced strategy in terms of geopolitical conflict. However, what happens in international relations can't be translated in terms of «win or lose.»

The balance of power in the world has changed, and we are moving fast towards a completely different structure. There is a rapid formation of one global society through the deployment of an information/cyber and communication revolution with the geostrategic information/cyber antagonism between leading countries of the world for achieving superiority in world cyberspace. It is time to strengthen our defenses against this growing danger to avoid the awful future! As Julian Borger said: «cyberwarfare: the great wild card that can turn the world's most advanced technology against itself with a few well-placed lines of code» [26].

References

1. Libicki M.C. Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND Corporation, 2009. – P. 17–24 [Web resource]. – Retrieved from: https://www.rand.org/pubs/monographs/MG877.html, open source (accessed on: 10.06.2017).

2. US Department of Defense et al. Joint Terminology for Cyberspace Operations. Washington DC, USA: Department of Defense, 2010–2011. – P. 28–30.

3. Clarke R.A. Cyber War: The Next Threat to National Security and What to Do about It / R.A. Clarke, R.K. Knake. – New York City, NY, USA: Harper Collins, 2010. – P. 235–258.

4. Vasilyeva I. The Value of Interaction for Russia, the USA and China Facing the Information Warfare// International Journal of Cyber Warfare and Terrorism (IJCWT). – Hershey, PA, USA: IGI Global, 2013. – Vol. 3, Is. 4. – P. 1–9 [Web resource]. – Retrieved from: http://www.igi-global.com/article/the-value-of-interaction-for-russia-the-usa-and-china-facing-the-information-warfare/105187, subscription (accessed on: 12.05.2017).

5. Vasilyeva I. Thirst for information: The growing pace of information warfare and strengthening positions of Russia, the USA and China / I. Vasilyeva, Y. Vasilyeva // Proceedings of the 8th International Conference on Information Warfare and Security, Denver, USA: Academic Conferences International Limited, 2013. – P. 215–220.

6. Center for Democracy and Technology et al. Comprehensive Privacy and Security: Critical for Health Information Technology. – Washington DC, USA: Center for Democracy and Technology, 2008. – Version 1.0. P. 1–4.

7. Center for Strategic and International Studies et al. Securing Cyberspace for the 44th Presidency // Commission on Cybersecurity for the 44th Presidency. – Washington DC, USA: Center for Strategic and International Studies, 2008. – P. 8–15 [Web resource]. Retrieved from: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf, open source (accessed on: 15.05.2017).

8. Council of Europe et al. Convention on Cybercrime/ European Treaty Series. – Budapest, Hungary: Council of Europe, 2004. – No. 185. – 5 p [Web resource]. Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561, open source (accessed on: 17.05.2017).

9. 111th Congress et al. Cybersecurity Act of 2010/ 111th Congress 2nd Session. – Washington DC, USA, 2010. – Calendar No. 707. – S. 773. – P. 2–13 [Web resource]. Retrieved from: https://www.congress.gov/111/bills/s773/BILLS-111s773rs.pdf, open source (accessed on: 17.05.2017).

10. Ozment A. Privacy Compliance Review of the Enhanced Cybersecurity Services (DHS/NPPD/PIA-028)/ US Department of Homeland Security. – Washington DC, USA: US Department of Homeland Security, 2015. – P. 6–12 [Web resource]. – Retrieved from: https://www.dhs.gov/sites/ default/files/publications/privacy-pcr-ecs-04102015.pdf, open source (accessed on: 18.05.2017).

11. Goode B. Privacy Impact Assessment Update for the Joint Cybersecurity Services Program, Defense Industrial Base

and Enhanced Cybersecurity Services (DHS/NPPD/PIA-021a)/ US Department of Homeland Security. – Washington DC, USA: US Department of Homeland Security, 2012 [Web resource]. – Retrieved from: https://www.dhs.gov/sites/ default/files/publications/privacy_pia_ice_livewave.pdf, open source (accessed on: 18.05.2017).

12. Goode B. Privacy Impact Assessment for the National Cybersecurity Protection System (DHS/NPPD/PIA-026)/ US Department of Homeland Security. – Washington DC, USA: US Department of Homeland Security, 2012 [Web resource]. – Retrieved from: https://www.dhs.gov/sites/ default/files/publications/privacy-pia-nppd-ncps-2015.pdf, open source (accessed on: 18.05.2017).

13. US Department of Defense et al. The Department of Defense Cyber Strategy. – Washington DC, USA: US Department of Defense, 2015. – P. 13–17, 24–30 [Web resource]. – Retrieved from: http://www.defense.gov/Portals/ 1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, open source (accessed on: 13.06.2017).

14. Sanger D.E. Pentagon Announces New Strategy for Cyberwarfare. – New York City, NY, USA: The New York Times, 2015 [Press]. Retrieved from: http://www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy.html, open source (assessed on: 13.06.2017).

15. US Armed Forces et al. Joint Publication 1, Doctrine for the Armed Forces of the United States. – Washington DC, USA: US Armed Forces, 2013. – [Web resource]. Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jp1.pdf, open source (accessed on 18.05.2017).

16. Weiguang S. Focus of Contemporary World Military Revolution – Introduction to Information Warfare. – China: The People's Liberation Army Daily (Jiefangjun bao), 1995. – P. 6–10.

17. Sharma A. Cyber Wars: A Paradigm Shift from Means to Ends// The Virtual Battlefield: Perspectives on Cyber Warfare. – Amsterdam, Netherlands: IOS press, 2009. – Vol. 3. – P. 3–17.

18. Boswell M. Media Relations in China's Military: The Case of the Ministry of National Defense Information Office. – Seattle, WA, USA: Asia Policy, 2009. – Vol. 8. – P. 97–120.

19. US Department of Defense et al. Annual Report to Congress: Military and Security Developments Involving the People's Republic of China. – Washington DC, USA: US Department of Defense, 2015.

20. Enze S. Logical Concepts of Information Warfare. – China: The People's Liberation Army Daily (Jiefangjun bao), 1996. – 135 p.

21. Clarke R.A. How China Steals Our Secrets. – New York City, NY, USA: The New York Times, 2012 [Press]. – Retrieved from: http://www.nytimes.com/2012/04/03/opinion/how-china-steals-our-secrets.html?_r=2&scp=2&sq=richard%20a%20clarke&st=cse&, open source (accessed on: 18.06.2017).

22. Oreku G. Cybercrime: Concerns, Challenges and Opportunities, Information Fusion for Cyber-Security Analytics/ G. Oreku, F. Mtenzi. – Switzerland: Springer International Publishing AG, 2016 – Vol. 691. – P. 129–153.

23. Spalding R. The New MAD World: A Cold War Strategy for Cyberwar / R. Spalding, A. Lowther. – USA: The National Interest Magazine, 2015 [Press]. – Retrieved from: http://www.nationalinterest.org/feature/the-new-mad-world-cold-war-strategy-cyberwar-13154, open source (accessed on: 18.06.2017).

24. Thornburgh, N. Inside the Chinese Hack Attack. – USA: Time Magazine, 2005 [Press]. – Retrieved from: http://content.time.com/time/nation/article/0,8599,1098371,00.html, open source (accessed on: 18.06.2017).

25. US Department of Defense et al. Annual Report to Congress: Military and Security Developments Involving the People's Republic of China. – Washington DC, USA: US Department of Defense, 2016.

26. Borger J. Trident is old technology: the brave new world of cyber warfare. – UK: The Guardian, 2016 [Press]. – Retrieved from: http://www.theguardian.com/technology/2016/jan/16/trident-old-technology-brave-new-world-cyber-warfare, open source (accessed on: 18.06.2017).

Vasilyeva Inna Sergeevna
Master of Science, Volgenau School of Engineering,
George Mason University, Fairfax, VA, USA.
Phone: +7-918-317-82-18
E-mail: inna1523@gmail.com

Васильева И.С.

США, Китай и основная концентрация на стратегической кибервойне

Текущая зависимость от информации и киберкомпонента сделала нашу цивилизацию гораздо более уязвимой. Скорость и широкое распространение информационных технологий и сетей вызвали огромный рост информационной и кибернетической силы оружия. С увеличивающейся ролью кибервойны в международной политике лидерство в киберсфере стало одним из основных способов достижения национальных стратегий. Будучи геополитическими противниками в достижении превосходства в мировом киберпространстве, США и Китай являются ключевыми лидерами на поле кибервойны. В статье раскрываются определение, исходные приоритеты кибервойны, а также развитие киберстратегий США и Китая, их баланс сил и будущее сосуществование.

Ключевые слова: кибервойна, безопасность, США, Китай, национальные стратегии, кибернетическое командование, информационная война.