THE RELATIONSHIP BETWEEN THE US AND CHINA IN THE CYBER SPACE

Dejan Vuletić, PhD, Research Associate
Strategic Research Institute, University of Defence, Serbia
dejan.vuletic@mod.gov.rs

Jovanka Šaranović, PhD, Research Associate
Strategic Research Institute, University of Defence, Serbia
jovanka.saranovic@mod.gov.rs

Assistant Professor **Ivan Vulić**, PhD,
University of Defence, Serbia
ivan.vulic@mod.gov.rs

Abstract: Modern society is critically dependent on information and information-communication technology. Information becomes increasingly important for national security, especially in the armed conflict. Modern conflicts are also strongly characterized as a battle in the information spectrum. Information-communication technology has created a new environment (cyber space), as well as the emergence of new resources and with them new ways of conducting conflicts. Such non-traditional attacks on information infrastructure could significantly jeopardize the military and economic power of the attacked state. In addition to the general considerations of cyber security, the paper presents some activities of the US and China in cyberspace as well as certain measures that they take to achieve domination in cyberspace.

Keywords: cyberspace, ralations, USA, China.

INTRODUCTION

Information-communication technology (ICT) has created a new environment (cyber space) that encompasses residents of any part of the world, of all age groups and social classes. Cultural, economic and life in general in the information society is critically dependent on information and information-communication technologies. The companies have been pulled, in all segments, into a race for information as key resources. In the information society, the raw materials are less and less valuable, while an increasing part of the value creation is done through information. As a result of accelerated growth and dependence on information and information-communication technology, vital national infrastructures are becoming increasingly automated and interconnected. The information provided by information and communication technology serves as a basis for making optimal decisions at all levels of society and contributes to the efficient utilization of the resources needed for the implementation of decisions.

Modern society critically dependens on information, as a strategic resource and information-communication technology, which carries out its transmission, processing or exchange of information (Vuletić, 2012). However, in addition to the advantages they provide, information has become an important goal of the opponent. In accordance with this, modern conflicts are characterized as fighting in the information spectrum. Domination in the information spectrum is a necessary condition for success and victory in the conflict. The new mode of engagement of states in the conflict has caused the emergence of new resources, and with them new ways of conducting the conflict (Vuletić, 2011).

CYBER SPACE AND CYBER SECURITY

The term "cyber space" consists of two words with a different meaning - cyber and space. In order to define the term "cyber space", it is necessary to determine the meaning of the word "cyber" and "space" (Vuletić, 2015). The cyber prefix refers to the term cybernetics. The word "cybernetics" comes from the ancient word *kybernao*, which in translation means to manage, in general terms. Although the roots of the word cyber can be seen in Viner's perceptions, the real meaning was given by William Gibson in his novel Neuromancer in 1984, where, under the term cyber, is meant - virtual, invisible, unlimited, technology-based. In the dictionary of Matica srpska, the "space" is defined as unlimited ambience, distance in all dimensions and directions (Rečnik srpskohrvatskog književnog jezika, 1973). The word 'space' has a different meaning in different scientific disciplines and hence it is difficult to find a universal, universally accepted definition.

Gibson sees the cyber space as the universe of computer networks, a world in which multinational companies, societies and other subjects struggle to conquer data and information. Under cyber space, it is understood that the type of community is composed of a computer network in which the elements of the classical society are in the form of bits and bytes, that is, the space created by computer networks. Cyber space is the term that connotate the online world of the Internet (computer networks), but also the digital world in general (Tipton & Krause, 2004). Vera Tasić and Ivan Bauer in the "Dictionary of Computer Terms" define the cyber space as a virtual reality environment (such as the Internet) in which people communicate using connected (networked) computers (Tasić & Bauer, 2003). In the Joint Publication (JP) 1-02 of the United States Department of Defense, a cyber space is defined as an unpredictable environment in which digital data is transmitted using computer networks (Joint Publication 1-02, 2010).

These definitions, in essence, connect the cyber space for computer networks. Cyber space, therefore, represents an immaterial, unlimited interactive space created by computer networks (Vuletić, 2017). Aljoša Mimica and Marija Bogdanović consider that cyber space is a new form of mental dimension of human existence within which a simulated reality arises as a result of the interaction between the human and artificial interface. It represents an alternative dimension within which a connection between different personal computers, computer networks, different virtual communities and individuals is established (Mimica & Bogdanović, 2007).

In everyday life, "cyber space" is commonly used as a synonym for the Internet. This identification is not entirely justified, because the global computer network, the Internet, is only part of the cyber space. However, the Internet is the largest information and communication system, both in terms of size and number of users. The Internet, therefore, has become a communication tool of global dimensions, with a basic and indisputable role in the economy and social life of all countries (Putnik, 2009). Cyber space represents a globally integrated information and communication infrastructure. It is an artificial creation created as a result of social needs and technological innovations.

Richard Coyne looks at the cyber space as a world (a set of physical entities eg hardware, communication lines), as space (objects can be close or far from each other so that distance can be measured) and as a place (for example, a website can be viewed as a site) (Coyne, 1995).

New technologies bring benefits as well as new problems, so that the use of ICT should be viewed as a "mix of benefits and disadvantages". New research highlights the threat that connected devices pose to critical infrastructure. Academics in Israel warned that it would be possible to hack internet-connected irrigation systems, turning these on remotely in order to drain a city's water reserves. A group of researchers from Princeton University found that a malicious botnet of water heaters and air conditioners could be used to manipulate the demand for energy by as much as 1%, leading to a blackout. These scenarios illustrate the challenge of securing critical infrastructure, suggesting that if industrial control systems are sufficiently hardened,

attackers will shift their focus to connected devices with weaker security standards (Critical infrastructure exploits, 2018).

According to Business Insider, hackers in Ireland, stymied by Apple's information systems security, are taking another approach to gain access to the corporation's data. They are offering Apple employees up to 20,000 euros for valid login credentials. While not all approaches to insiders are so overt, this case nevertheless serves as a great reminder that malicious actors are actively recruiting insiders to exploit their status. Beyond that, it demonstrates that the insider threat is not just confined to an Edward Snowden type who steals a mass of data in one swoop before leaving the company. Insiders can pose a far more subtle and enduring threat (When Cyber Security Is an Inside Threat, 2016).

A massive ransomware[1] attack affecting more than 70 countries took place on May 12 2017. Over 36,000 Wannacrypt (Wanna Decryptor virus) cases have been detected globally in the United States, Russia, Spain, Turkey and the United Kingdom. The attack struck targets as diverse as the Russian Ministry of the Interior, the British National Health Service, Reuters news agency and Spain's largest telecom firm, Telefonica. A number of European banks were also affected. Ransomware is an increasingly common cyber threat. Similar large-scale attacks already occurring and will likely become more common in the future (Global: Massive Ransomware Attack Goes Viral, 2017).

The mentioned and other numerous incidents in cyber space show that the protection of information communication resources is becoming one of the priorities of national security. The protection of information communication resources is becoming one of the priorities of national security. Cyber security is defined and understood in different ways. In a narrow and technical sense, cyber security has been defined as the ability to control access to network systems and the information they contain (Nissenbaum, 2005). The cyber security concept has also gained a national security dimension as the public, businesses and the military have become increasingly dependent on computer and networked technologies.

Cyber crime generates cost for national economies. In a report by McAfee and the Centre for Strategic and International Studies (CSIS), the annual cost of cyber crime to the global economy was estimated to be more than $400 billion. It's a global average loss of 0.5 per cent of gross domestic product (Net Losses: Estimating the Global Cost of Cybercrime, 2014). Research shows that developing countries are most vulnerable to cyber threats. Wealthier countries have higher levels of Internet connectivity, and hence the people, businesses and institutions in those countries are more likely to be affected by cyber crime (Kaspersky Lab, 2014).

Geopolitical disagreements spill over into cyber space (e.g. Estonia in 2007 - disruption of the functioning of government and computer networks of the banking sector, Georgia 2008 - attack on computer networks and government sites, Sweden in 2009 - disruption of the functioning of websites and computer networks of banks, police and other government institutions).

USA AND CHINA IN CYBER SPACE

World powers, e.g. The United States and China views cyber space as the new, fifth, warfare area. Speaking at DEF CON 2018, senior National Security Agency (NSA) official and former White House Cyber security Coordinator Rob Joyce outlined his perspective on the state of cyber security. Joyce specifically called out four nations – China, Iran, North Korea and Russia – for irresponsible behaviour on the internet (NSA calls out adversary cyber activity, 2018).

[1] Ransomware is a type of malicious software that forcibly encrypts data on a targeted system, usually requiring a ransom to be paid in return for decrypting the information. If the ransom (in bitcoins) isn't paid, then the data is invariably wiped.

Numerous cases indicate an endeavor or race between the United States and China for economic and technological supremacy. One of the main arenas for this competition is cyber space (China Won't Back Down on Cyber Espionage Anytime Soon, 2018). The US Department of Defense (DoD) has released a summary of its 2018 Cyber Strategy that highlights Russia and China as long-term threats to the US. The Stategy states that the Department must take action in cyber space during day-to-day competition to preserve US military advantages and to defend US interests. This DoD summary, which focuses on deterring malicious cyber activities, defending critical infrastructures and strengthening the security in cyber space, does not adequately predict the features of information conflict through cyber space (Director's cut - Insight from Sean Kanuck, 2018).

At the cyber security conference "Zero Day Con", Defense Intelligence Agency Director Lt-Gen Robert Ashley highlighted the intersection between great-power competition and cyber power. Top US officials have also expressed growing concerns over what Secretary of Homeland Security Kirstjen Nielsen and Vice President Mike Pence have called "unprecedented efforts" by China to compromise US interests. In his speech on 4 October 2018, Pence denounced China's growing aggression, referencing its expanding civilian surveillance programme and continued theft of US technology. Some analysts believe that after a reduction in activity in 2016, China has restored efforts to use methods of cyber espionage and hacking "against Western industry". Such responses come on the heels of the extradition, and pending prosecution, of Chinese intelligence official Yanjun Xan (Great power cyber competition, 2018).

The US Department of Justice announced the creation of a multi-departmental task force to counter Chinese economic espionage. In a speech, then-Attorney General Jeff Sessions cited incidents such as the indictment of a Chinese state-owned company, Fujian Jinhua Circuit Co Ltd, for allegedly stealing intellectual property from US firm Micron Technology Inc. The Chinese company and affiliated entities were added to the US Department of Commerce's "entity list", which prevents them from trading in any US patented technological goods. These moves follow charges brought against ten Chinese nationals for a cyber espionage campaign against US aerospace companies (NSA calls out adversary cyber activity, 2018).

US investigators allegedly discovered that Chinese People's Liberation Army operatives inserted spyware microchips into US hardware during the manufacturing process in China. The microchips were found inside devices produced by Supermicro, one of the largest suppliers of server motherboards. With memory, network capabilities and advanced processing power, chips the size of a pencil tip created a backdoor to any network connected to the affected devices. Almost 30 companies were affected by the breach, including Amazon and Apple. (Chinese firmware compromises US tech supply chain, 2018).

China is taking extensive steps to present itself as a viable cyber security partner and all-round good global cyber-citizen. The exploitation of cyberspace meets a critical need in terms of China's core strategic objectives. China aims to continue establishing itself as a major regional and global power. The last several 5-year-plans identify the development of key strategic emerging industries as a major component. That include, among other, the development of information-communication technology. Cyber espionage is useful tool to obtaing valuable information and avoiding an open conflict. Strategic emerging industries are prominent targets of cyber-attacks. Despite any international commitments it is unlikely that countries intend to give up or reduce exploitation of cyber space. China's interest in bilateral agreements and international norms is best understood as something between smokescreen and stalling strategy. By engaging internationally and securing bilateral agreements, China mitigates or avoids negative costs (political, diplomatic and economic) attached to its widespread cyber espionage, while also utilising the process of engagement to delay the development and implementation of effective counter-strategies while the benefits accrue. International engagement and agreements bolster China's legal standing and promote China as a viable cyber security partner (Sawers, 2018).

That effort is more important to China as the internet becomes more essential to China's economy. In 2015 Premier Li Keqiang launched the "Internet Plus initiative", a plan to incorporate the internet across nearly all sectors of the Chinese economy. The central government hopes that the integration campaign will enable China to collect an unrivaled store of data that it can use to strengthen its networks and technologies (China Won't Back Down on Cyber Espionage Anytime Soon, 2018). As China increasingly gains the economic benefits of global connectivity, the West's technological edge is fast eroding. China's emergence as a major global power is reshaping the cyber domain. The country has the world's largest internet-user community, a growing economic footprint and increasingly capable military and intelligence services (China's Cyber Power, 2016).

Despite the criticisms of China's offensive actions, such as industrial espionage, China's cyber security policy focuses predominantly on defensive strategy. China is concerned that outside rivals such as the United States could invade its cyber space to spread disinformation or subvert the state through asymmetric attacks. In fact, it views the internet as a tool that the United States has created to exploit to its benefit. It's hardly surprising, then, that one of the main priorities behind China's internet strategy is keeping unwanted information and intruders out of its cyber space with the Great Firewall (China Won't Back Down on Cyber Espionage Anytime Soon, 2018).

China tries to control and disconnect, optionally, the country from internet and and uses its own technology. The plan is as much a strategic initiative as an economic one, and it will help the central government protect China from its rivals, both at home and abroad. China enacted a cyber security law in 2017 that gives the government a legal basis for forcing foreign companies to relinquish control of their data and to submit source code for review (China Won't Back Down on Cyber Espionage Anytime Soon, 2018). The Cyberspace Administration of China issued stricter rules for internet companies. The rules call for companies to increase policing efforts of online speech, regularly report on 'harmful' content and maintain extensive user records (Asian countries tighten control of internet, 2018).

The fact is that the United States and China will continue using the internet and cyber space against each other. A 2015 agreement stipulating that neither would engage in cyber espionage to steal trade secrets or intellectual property from the other has reduced but apparently not eliminated these practices. In November 2017, the United States charged three Chinese hackers working at an internet security firm based in China with eight separate counts of conspiring to commit computer fraud and trade secret theft. The current U.S. administration takes aim at China's economic and industrial strategies through tariffs and trade investigations, China will use cyber space to insulate itself from the United States (China Won't Back Down on Cyber Espionage Anytime Soon, 2018).

China has the capabilities and the will to surpass the West in military capability. However, no one is sure how far China's current strengths, long-term plans, technical solutions, achievements in the field of ICT (The Uncertain Future of Warfare, 2018). China is the country with the economic and military capacity to truly challenge the United States and to disrupt the international system it presides over. The internet is an increasingly critical part of that system. Consequently, cyber space will be an important battlefield between U.S. and China (China Won't Back Down on Cyber Espionage Anytime Soon, 2018).

CYBER WAR (WARFARE) STRENGTH

Cyber Warfare is a type of hostile activity undertaken against computer networks, computer systems and databases with the goal of degrading or destroying targeted systems. In this way, targeted systems can be unusable, degraded performance, which can affect the commander to make a bad decision due to lack of information. The cyber warfare is as an unauthorized access in computers or networks of another nation, or undertaking other activities affecting the computer

system with the aim of adding, modifying or falsifying data or causing interruptions or damage to computers, network devices or objects for controlling computer systems. Libicky thinks that cyber attack deliberately disables or removes the computer systems of a subject by another subject (Libicki, 2009). The attacking entity may be a national or non-state actor. The cyber warfare, therefore, is a form of information warfare that consists of a series of actions that break down or destroy the information-communication systems of the opponent (for example, insertion computer viruses in the opponent's military systems). Mark cyber attack as cyber crime, terrorism or otherwise somewhat disputable because it is difficult to determine the identity, intent, or political motivation of the attackers.

In addition to the US, Russia and China, there are between 20 and 30 countries with respectable cyber warfare capabilities (Clarke & Knake, 2010). The United States has the most sophisticated and most complex cyber warfare capabilities, followed by Russia and China. The United States is likely to possess the most sophisticated offensive capabilities for cyber warfare, but there are some weaknesses when it comes to defense. China has devoted much more attention to the defense all national networks. In China, networks that comprise Chinese infrastructure are controlled by the government either through direct ownership or through a close partnership with the private sector. China has the power to disconnect "their part" of cyber space from the rest of the world, which they can do in the eventual conflict. The United States does not have such capabilities (Paul 2008).

The United States is currently far more vulnerable to cyber attacks than China and Russia. The eventual cyber war at the moment is a drawback for the US, cyber security experts say. Measurement of cyber war strength, in addition to the offensive aspect, also implies defense (a measure of national capacity to take action if attacked, actions that will block or mitigate the attack) and dependency (reliance on computer networks and systems that can be vulnerable to cyber attacks). Measurement of cyber war strength, Clarke and Knake have been based on the assessment of offensive power, defensive capabilities and computer system dependencies. Dependence refers to critical information systems that do not have a real substitute that depend on cyber space. A smaller dependent nation gets a higher score when ranked (Clarke & Knake, 2010).

According of their measurement:

- U.S. – total 11
  Cyber Offense: 8
  Cyber Dependence: 2
  Cyber Defense: 1

- China – total 15
  Cyber Offense: 5
  Cyber Dependence: 4
  Cyber Defense: 6

China has a high score for defense because it has the plan and ability to disconnect national networks from the rest of the cyber space. In the opinion of Clarke and Knake, the United States does not have this possibility.

CONCLUSION

Modern society is characterized by the increasing use of information-communication technology. Most countries have essential resources based on information and communication technology, including defense systems and infrastructures that include control of electricity, telephone system, money flows, air transport, oil, gas and other information-dependent areas. In

this context, it must be understood that future enemies, either states, groups or individuals, can try to endanger these infrastructures by using non-traditional methods, and such non-traditional attacks against information infrastructure could significantly jeopardize the military and economic power of the attacked state. Accordingly, the information revolution and associated organizational and functional changes alter even the nature of the conflict.

The information revolution cause changes in how societies will be able to come to conflict and how their armed forces will be able to lead an armed conflict. The development and expansion of information-communication technology will significantly change the conduct of military operations. These changes in the information environment make information superiority a key enabling factor in the evolution of the operational capabilities of the armed forces. The evolution of information-communication technology will enable the integration of the traditional form of information operations with sophisticated intelligence activity of all sources, observation and reconnaissance in a fully synchronized information campaign.

Society becomes increasingly dependent on ICT, which will lead to its increasing sensitivity due to an increasing number of users of information-communication technology and the trend of interconnection of computer networks. Strategic importance is the identification of critical national infrastructures that can be endangered, the constant exchange of information and experiences as well as cooperation between the private and the state sector.

Cyber attacks against states are becoming more numerous and more serious. Military presence in cyberspace is undoubtedly. Numerous examples show that for complex, coordinated attacks, it takes several years of preparation.

The future of cyber will depend on the future of vulnerabilities, especially the development of the internet of things (IoT). The future of cyber will depend on the future of vulnerabilities, especially the development of the internet of things (IoT). The digital revolution has produced a new warfare domain in which to spy, sabotage and prepare the battlefield. Some experts think that the worst gaps in defenses have been filled. A new generation of military and civilian leaders seems increasingly aware of the seriousness of the problem. (The Uncertain Future of Warfare, 2018). China's ability to cyber warfare is on a constant growth. China has the knowledge and ability to overcome the US in the future and become the world's leading power in cyber space.

REFERENCES

1. *Asian countries tighten control of internet* (2018), Downloaded February 23, 2019, *https://www.iiss.org/blogs/cyber-report/2018/11/cyber-report-16-to-22-november*
2. Clarke, R. & Knake, R. (2010). *Cyber War – The next threat to National Security and What to do about it.* Pymble, Australia: HarperCollins Publishers.
3. *China's Cyber Power* (2016), Downloaded February 20, 2019, *https://www.iiss.org/publications/adelphi/2016/chinas-cyber-power*
4. *China Won't Back Down on Cyber Espionage Anytime Soon* (2018), Texas, USA: Stratfor Global Intelligence.
5. *Chinese firmware compromises US tech supply chain* (2018), Downloaded February 16, 2019, *https://www.iiss.org/blogs/cyber-report/2018/10/cyber-report-28-september-to-4-october*
6. Coyne, R. (1995). *Designing information technology in the postmodern age: From method to metaphor*. Cambridge, USA: MIT Press.
7. *Critical infrastructure exploits* (2018), Downloaded April 18, 2019, *https://www.iiss.org/blogs/cyber-report/2018/08/cyber-report-17-to-23-august*
8. *Director's cut - Insight from Sean Kanuck* (2018), Downloaded April 3, 2019, *https://www.iiss.org/blogs/cyber-report/2018/09/cyber-report-14-to-20-september*
9. *Global: Massive Ransomware Attack Goes Viral* (2017), Texas, USA: Stratfor Global Intelligence.

10. *Great power cyber competition* (2018), Downloaded March 17, 2019, https://www.iiss.org/blogs/cyber-report/2018/10/cyber-report-12-to-18-october
11. *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms* (2010), Downloaded April 14, 2019, https://fas.org/irp/doddir/dod/jp1_02.pdf
12. *Kaspersky security bulletin* (2014), Downloaded May 13, 2019, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08065515/Kaspersky-Security-Bulletin-2014-EN.pdf
13. Libicki, M. (2009). *Cyberdeterrence and Cyberwar.* California, USA: RAMD Corporation.
14. Mimica, A. & Bogdanović, M. (2007), *Sociološki rečnik*. Beograd: Zavod za udžbenike.
15. *Net Losses: Estimating the Global Cost of Cybercrime* (2014), Washington, USA: Center for Strategic and International Studies.
16. Nissenbaum, H. (2005). Where computer security meets national security, *Ethics and Information Technology*, 7 (2), pp. 61-73.
17. *NSA calls out adversary cyber activity* (2018), Downloaded April 16, 2019, https://www.iiss.org/blogs/cyber-report/2018/08/cyber-report-9-to-16-august
18. Paul, C. (2008). *Information Operations – Doctrine and Practice*. London, United Kingdom: Praeger Security International.
19. Putnik, N. (2009). *Sajber prostor i bezbednosni izazovi*. Beograd: Fakultet bezbednosti.
20. *Rečnik srpskohrvatskog književnog jezika* (1973). Novi Sad: Matica srpska.
21. Sawers, M. (2018), *How Beijing's Cyber Security Engagement Incorporates the Three Warfares*, Texas, USA: Stratfor Global Intelligence.
22. Tasić, V. & Bauer, I. (2003). *Rečnik kompjuterskih termina*. Beograd: Mikro knjiga.
23. Tipton, H. & Krause, M. (2004). *Information Security Management Handbook (fifth edition)*. New York: CRC Press.
24. *The Uncertain Future of Warfare* (2018), Texas, USA: Stratfor Global Intelligence.
25. Vuletić, D. (2012). *Bezbednost u sajber prostoru*. Beograd: Medija centar "Odbrana".
26. Vuletić, D. (2011). *Odbrana od pretnji u sajber prostoru*. Beograd: Institut za strategijska istraživanja.
27. Vuletić, D. (2017). *Sajber bezbednost*, In: B. Forca (Ed.),Integralna bezbednost Republike Srbije, pp. 169-184, Beograd: Univerzitet "Union-Nikola Tesla".
28. Vuletić, D. (2015). *Sajber terorizam*, In: Grupa autora, *Savremeni terorizam*, pp. 263-330, Beograd: Institut za medjunarodnu politiku i privredu and Javno preduzece "Sluzbeni glasnik".
29. *When Cyber Security Is an Inside Threat* (2016), Texas, USA: Stratfor Global Intelligence.