DOI: 10.22363/2313-0660-2017-17-2-339-348

THE ROLE OF CYBERSECURITY IN WORLD POLITICS

V.T. Tsakanyan

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

Abstract. The purpose of this paper is to investigate a significant and increasing role of cybersecurity in world politics. Cybersecurity threats are one of the main national security, public safety, and economic challenges every nation faces in XXI century. Cyberspace is a defining feature of modern life. Individuals and communities worldwide connect, socialize, and organize themselves in and through cyberspace. The existence of numerous cyber security issues on various spheres of life naturally increase political interest in resolving them. The need for cybersecurity is growing ranging from particular cases to national and international — becoming the main problem of diplomacy and world politics.

Based on the different national approaches, cybersecurity is seen as the instrument to gain national interests. All countries believe that cybersecurity is an instrument to achieve state's national interest, since more of the modern theories are focus in the material gain. Meanwhile, some countries see cybersecurity as the tool to influence the adversaries' perception. This condition build based on the enormous destruction power of cyberattacks. In contrast with the two main approaches, the national security institutions emphasize to the idea, not the material gain. The difference between these national security approaches is the way to use this instrument is used in order to gain the objectives. Indeed, cybersecurity has an important and special role in the world politics.

Key words: Cybersecurity, information security, national security, world politics, United States of America, Russian Federation, People's Republic of China, UN

The meaning of "security" is often treated as a common-sense term that can be understood by "unacknowledged consensus" [Sheehan 2005]. The content of international security has expanded over the years. Today it covers a variety of interconnected issues in the world that affect survival. It ranges from the traditional or conventional modes of military power, the causes and consequences of war between states, economic strength, to ethnic, religious and ideological conflicts, trade and economic conflicts, energy supplies, science and technology, food, as well as threats to human security and the stability of states from environmental degradation, infectious diseases, climate change and the activities of non-state actors [Buzan, Wæver 1998].

The so-called interwar revolution saw the advent of combined-arms, mechanized air-land operations (blitzkrieg), the displacement of the line of battle at sea by fast carrier task forces, the rise of long-range strategic aerial bombardment, and the introduction of in targeted air defense networks. Later, World War II witnessed the introduction of nuclear weapons, as well as cruise and ballistic missiles, which triggered and other fundamental change in the character of warfare [For a discussion... 1996].

Because traditional notions of security focused on the use of force between great powers, the focus of international security studied during the Cold War was naturally on superpower conflict and nuclear war. With the end of the Cold War, analysts began to argue that the subject of international security "had to be recast to reflect the changing nature of conflict" [Freedman 1998].

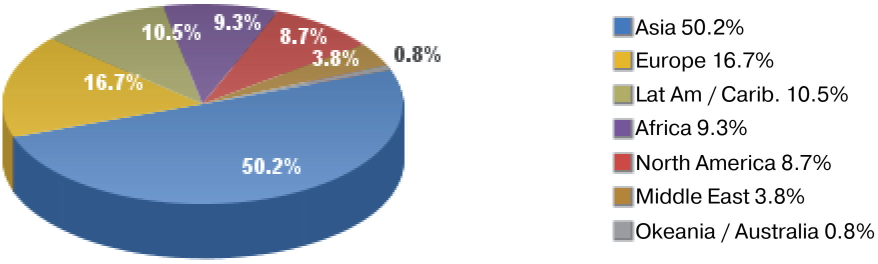
As the Internet experienced its rapid expansion in the 1990s, hackers began engaging in cyber "pranks" while low-level criminals began exploring the potential for cybercrime. Once it was shown that "crime pays" in the cyber domain, organized crime began muscling its way onto the scene, in some cases apparently with the blessing — and even support — of the governments on whose territory they were operating [Weiss 1996].

The paper begins with from discussing the approaches that give the explanation about the role of the cyberspace in world politics. It discusses the views of the various national security doctrines.

The United States, along with Western Europe and Japan first made the transition to an information society. Already in the early 1970s, the dominant part of the workforce (70%) was in these countries are concentrated in the services sector and consisted of "information workers" [Bell 1979].

Information warfare covers a very wide range of activities in the information space, from attacks on communication systems and critical infrastructure and ending with the use of ICT for implementation of techniques of psychological impact [Arquilla 1999].

ICT today form the basis of a rapidly developing global information society. Global network the Internet covers about 3.6 billion people (approximately 49.5% of the world population)[1].



Internet Users in the World by Regions June 2016

Source: Internet World Stats — www.internetworldstats.com/stats.htm
Basis: 3,675,824,813 Internet users on June 30, 2016
© Miniwatts Marketing Group, 2016

Actively developing the "Internet of things" that binds not only people, but also to network, computer devices, appliances and other items. According to forecasts, in 2020 about 50 billion devices will have an Internet connection[2].

Former President of the Corporation for the domain name and ICANN IP-address management (Internet Corporation on Assigning Names and Numbers) R. Beckstrom articulated three key principles with respect to the Internet:

1) all that has Internet access can be "hacked";

2) all have access to the Internet;

[1] Internet World Stats. Usage and Population Statistics. URL: http://www.internetworldstats.com/stats.htm (accessed: 12.01.2017).

[2] Ericsson CEO to shareholders: 50 billion connections 2020. April 13, 2010 URL: http://www.ericsson.com/thecompany/press/releases/2010/04/1403231 (accessed: 12.01.2017).

3) in this way, everything becomes vulnerable. The world is entering a phase of the endless struggle against cyber threats that are constantly updated[3].

In May 2007, the European Commission issued a Communication “towards a general policy on the against cybercrime”, noting that there was not even an agreed definition of cybercrime [Anderson et al. 2012].

It proposed a threefold definition:

1) traditional forms of crime such as fraud or forgery, though committed over electronic communication networks and information systems;

2) the publication of illegal content over electronic media (e.g., child sexual abuse material or incitement to racial hatred);

3) crimes unique to electronic networks, e.g., attacks against information systems, denial of service and hacking.

The protection of lives and property from foreign actors is a universally understood role of government, and the cyber era introduces new capacities for other nations to wage war. As cyberlaw theorist Paul Rosenzweig points out, just as everyone would expect the government to defend against enemy aircraft rather than leaving it to each individual or enterprise, so too would we expect the imperative of “the common defense” to extend into cyberspace [Rosenzweig 2010].

This also includes the threat of non-state actors targeting civilian infrastructure for political gain, even if the threat of cyberterrorism is perhaps overstated [Singer, Friedman 2014].

Deterring and countering these types of threat and maintaining security in cyberspace involves a number of actors spread across the public and private sectors, as well as society as a whole. Examples of the breadth of actors involved in response include [Robinson et al. 2012]:

♦ national-level policy units with responsibility for cyber-securityissues — for example, the Office of Cyber Security and Information Assurance (OCSIA) in the UK, and Estonian Authority for Information Systems (RIA) in Estonia;

♦ national-level coordinatingunits or institutions with responsibility for critical national infrastructure protection missions — e.g. Centre for the Protection of National Infrastructurein the UK, and National Infrastructure Coordinating Center in the Netherlands;

♦ specific inter-governmental units dedicated to national cyber-defence missions — for example, the Cyber Security Operations Centre in the UK;

♦ operational agencies — intelligence, armed forces and law enforcement authorities — agencies which may be involved in the delivery of elements of the state’s cyber capability: cyber deterrence, cyber-warfare, investigation, countering or investigating cybercrime, for example USCYBERCOM and theNational Security Agencyin the USA;

♦ national and/or governmental computer emergency response teams (CERTs) — types of CERT which collate and receive information from other CERTs with whom they have a peer relationship, but have a specific role to play in protection of the critical information infrastructure;

[3] Beckstrom, Rob. Speech at the London Conference on Cyberspace [electronic resource] / ICANN. November 2, 2011. URL: https://www.icann.org/en/system/files/files/beckstrom-speech-cybersecurity-london-02nov11en.pdf (accessed: 12.01.2017).

♦ communication service providers responsible in varying ways for parts of the infrastructure which make up 'cyberspace' — they may include 'essential' providers, which provide backbone, long-haul interconnectivity to mobile network operators or retail internet service providers. Some forms of provider may even be 'virtual' resellers of bandwidth or access to different markets (for example, BT and C&W in the UK, Verizon in the USA);

♦ infrastructure hardware providers such as Cisco, Juniper Networks or Huawei — these companies manufacture the hardware andmiddleware and provide software for the infrastructure. Some such companies also have a systems integration role, which can have security implications when the nationality of the company (e.g. Huawei) may not be a close ally, or essential intellectual property for critical national infrastructure is unobtainable (US companies);

♦ Software and services providers whichdesign, develop, produce and market software — such firms may specialize, for example, in cryptographic software, infrastructure or services, and other industry firms including those in the integrated semi-conductor industry which design microchips (e.g. ARM or Intel) [Robinson et al. 2012].

Thus, Dorothy Denning, one of the most authoritative experts on cyberterrorism, defines this concept as "illegal attacks or threats of an attack directed against computers, networks and information stored in them to intimidate or coerce the government and the population of the country to achieve political or social goals" [Denning 2000].

MAIN APPROACHES

This section discusses the role of cybersecurity in world politics based on the approaches from the USA, Russia and China. It explains the capacity of cybersecurity in world politics according to these approaches. It addresses the following questions: How cybersecurity affects the relations among the states? What kinds of role are played by cyberspace?

UNITED STATES OF AMERICA

The United States, being the leaders in the field of ICT, among the first to encounter the negative consequences of the information revolution. To date, the US experience in the field of information security is an advanced, which leads to the relevance and importance of the study.

In 1991, the United States formulated the concept of Revolution in Military Affairs, characterized by extensive use of ICT to provide management, control and intelligence, information wars, and the use of various types of non-lethal weapons [Metz, Kievit 1995].

Economy and national security of the US today are totally dependent on information technology and information infrastructure. Network technologies ensure the functioning of the US critical infrastructure in sectors such as energy, transport, banking and finance, information and telecommunications, health care, emergency services, agriculture, nutrition, water, military and industrial base, chemical products and hazardous materials, mail and delivery services.

Federal Bureau of Investigation (FBI) in its activities based on the subjective approach and identifies three main groups of actors that pose a threat in cyberspace:

1) organized crime groups that are most prone to the financial services sector and constantly improve cyber power;

2) states sponsors who are interested in stealing data, including intellectual property, research, and development of enterprises, public institutions and contractors;

3) terrorist groups using network technology to conduct destructive actions against the country of critical infrastructure, and thus pose a threat to US national security[4].

In turn, within the framework of international discussions on the US IIB offer consider the following four sources of threats to cyber security: the criminals, the state terrorists, as well as intermediaries (individuals or groups carrying out malicious network activity on behalf of others — whether state or non-state actors — to financial gain, or on the basis of nationalist or other political motives)[5].

The US Department of Defense (DoD) in its activities based on the four categories of threats to cyber security, which include both the actors and the individual steps: — the threats posed by external actors (foreign governments, criminal groups); — Threats from internal actors (insiders); — Threats associated with the vulnerability of the network of suppliers of equipment and software; — Threats to the functional activity of the Ministry[6].

RUSSIAN FEDERATION

The problem of legal regulation of cybersecurity in the Russian Federation is an organic component of the state policy of development of the national sector of information technologies [Matveev 2014].

Among the documents that define today the fundamental approaches to information security in the Russian Federation, can be distinguished, first of all, the following:

♦ Law of the Russian Federation of 27.07.2006 number 149-FL “On Information, Information Technologies and Protection of Information”;

♦ Fundamentals of the Russian Federation's state policy in the field of international information security for the period up to 2020;

♦ The doctrine of national information security;

♦ Strategy for Information Society Development in the Russian Federation. These, as well as accompanying departmental normative documents (primarily documents FSTEC Russia) today form an integrated system requirements for information security for the information systems of different levels. At the same time clarifying the specifics of the issue of cyberspace, as well as relevant threats and protection mechanisms certainly deserves special consideration.

[4] The Cyber Threat (Shawn Henry): Part 1. On the Front Lines with Shawn Henry. Federal Bureau of Investigation. March 27, 2012. URL: http://www.fbi.gov/news/stories/2012/march/shawn-henry_032712 (accessed: 12.03.2014).

[5] Developments in the field of information and telecommunications in the context of international security. Report of the UN Secretary General. Document A / 66/152 of 15 July 2011. P. 18—20. URL: http://www.un.org/ru/documents/ods.asp?m=A/66/152 (accessed: 03.12.2014).

[6] Department of Defense Strategy for Operating in Cyberspace. July 2011. P. 3. URL: http://www.defense.gov/news/d20110714cyber.pdf (accessed: 03.12.2014).

The modern legal instruments in the field of cyber security should emphasize the following:

- ♦ Conceptual views on the activities of the Armed Forces in the information space;
- ♦ Draft Law "On the security of the Russian Federation of the critical information infrastructure" [Chobanyan, chalahami 2013];
- ♦ Decree of the President of Russia 2013. Number 31c "On establishment of the state detection, prevention and response to cyberattacks on information resources of the Russian Federation".

According to the Cyber Security Strategy of Russian Federation, the Strategy of cyberspace should be regarded as certain, having a clear boundary element information space. This approach is consistent with international standards, which give definition to the terms of the information security sector and establish their relationship. "Cyber-security" is meant, thus, a narrower in the sense of the concept than the "information security".

The strategy is based on the key principles of the Federal Law on 27.07.2006 No 149 Federal Law "On information, information technologies and information protection".

1. To which security can be attributed Russian Federation in creation of information systems, their operation, and privacy of non-collection, storage, use and dissemination of information about the private life of a person without his consent.

2. The strategy is consistent with the doctrine of the Russian information security oh Federation (doctrine) and develops its individual provisions. One of the central tasks in the field of information security.

According to the doctrine, it is the development of criteria and evaluation methods the effectiveness of systems and information security. The strategy provides for action to ensure the safety government information resources, such as holding regular assessment of security of state information resources and systems[7].

The main governmental actors in Russian Federation which are engaged to national cybersecurity systems are:

- ♦ Government of the Russian Federation (2009) Russia's national security strategy to 2020[8];
- ♦ Government of the Russian Federation, Ministry of Defense (2011) Convention on international information security[9];
- ♦ Government of the Russian Federation (2000) Information security doctrine of the Russian Federation[10].

Both in the Russian Federation and China cyber security is seen as a component of information security, including the promotion and impact on population.

[7] Cyber Security Strategy of Russian Federation (Concept). URL: http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (accessed: 12.01.2017).

[8] Wikidot. URl: http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020 (accessed: 12.01.2017).

[9] Ministry of Foreign Affairs of Russia. Resource. URL: http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument (accessed: 12.01.2017).

[10] Ministry of Foreign Affairs of Russia resource. URL: http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d90 (accessed: 12.01.2017).

PEOPLE'S REPUBLIC OF CHINA

The Chinese government perceives software by Western manufacturers as a threat to national security. Therefore, its use in China is strictly regulated. The international implications of this regimentation are already becoming apparent. Chinese cyber security policy in general has the potential to alter the global market for IT products and services fundamentally. China's government is currently taking concrete steps to enhance cyber security: in the spring of 2014, it founded the "Central Cyber Security and Informatization Leading Group" (中央网络安全和信息化领导小组).

"NO NATIONAL SECURITY WITHOUT CYBER SECURITY"

"No national security without cyber security" (没有网络安全就没有国家安全), said President Xi Jinping to the state-run news agency Xinhua in April 2014.

Over the last few years, though, problems in implementing cybersecurity policy have not been restricted to China alone. Other countries are also having trouble, albeit in different areas. In Germany, for example, cybersecurity still is not a central political issue. Measures enacted by the federal government such as introducing a "nospying" provision or setting up a new, independent communications network for the federal government alone are considered by IT experts and public authorities such as the German Federal Audit Office to be half-hearted and ineffective[11].

Due to the different approaches to ensure national security and because of the different understanding of the security issues, there is no common approach in world politics as agreed in cyberspace. States are trying to establish bilateral agreements Compliance Assistance in cyberspace. One of the existing methods of matching approaches to cyber security are UN resolutions.

Recalling also its resolutions on the role of science and technology in the expressing its concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields, confirming the request to the Secretary-General contained in paragraph 4 of its resolutions 56/19 and 57/53.

1. Calls upon Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information.

2. Considers that the purpose of such measures could be served through the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems.

[11] Jaume-Palasí, Lorena and Gierow, Hauke (2014). "Germany", in: Davies, Simon (ed.). "A Crisis of ccountability: A global analysis of the impact of the Snowden revelations". P. 42—46. http://www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf (accessed: 12.01.2017).

3. Invites all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) general appreciation of the issues of information security;

(b) definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources;

(c) the content of the concepts mentioned in paragraph 2 of the present resolution.

4. Requests the Secretary-General to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them, and to conduct a study on the concepts referred to in paragraph 2 of the present resolution, with the assistance of a group of governmental experts, to be established in 2004, appointed by him on the basis of equitable geographical distribution and with the help of Member States in a position to render such assistance, and to submit a report on the outcome of the study to the General Assembly at its sixtieth session.

5. Decides to include in the provisional agenda of its fifty-ninth session the item entitled Developments in the field of information and telecommunications in the context of international security[12].

The first — an approach the United States and its allies, according to which for cybersecurity at the international level does not require the development and adoption of new rules and principles. According to this approach, the basis of ensuring cybersecurity regime form the UNGA Resolution on combating the criminal misuse of information technology and global culture of cyber security, the UN Security Council resolutions, the provisions of which are aimed at combating terrorism, as well as the provisions of the Council of Europe Convention on Cybercrime. In turn, the UN Charter and existing principles of international law provide the necessary framework for the regulation of activities of States in the use of ICT in the military-political purposes. It is important to emphasize that the US approach focuses on the development of international mechanisms of information security in the narrow sense — cybersecurity. The second — the approach of the Russian Federation and its partners, which are based on the need to develop, taking into account the specifics of the information space of a special regime in the form of the UN Convention on ensuring international information security. The proposed draft document covers the full range of information security threats (military-political, criminal and terrorist nature), including such important from the point of view of the national interests of the Russian threat, as the action in the information space in order to undermine the political, economic and social systems of other states, psychological treatment population, destabilizing society and the manipulation of information flow in the information space of other countries.

[12] Resolution adopted by the General Assembly on 8 December 2003 [on the report of the First Committee (A/58/457)] 58/32. Developments in the field of information and telecommunications in the context of international securityhttps://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/454/83/PDF/N0345483.pdf (accessed: 04/20/14).

***

In conclusion, based on these approaches, cybersecurity is seen as the instrument to gain national interests. All countries believe that cybersecurity is an instrument to achieve state's national interest, since both of the theories are focus in the material gain. Meanwhile, some countries see cybersecurity as the tool to influence the adversaries' perception. This condition based on the enormous destruction power of cyberattacks. In contrast with the two previous approaches, the national security institutions emphasize to the idea, not the material gain. The difference between these national security approaches is the way to use this instrument is used in order to gain the objectives. Indeed, cybersecurity has an important and special role in the world politics.

REFERENCES

Anderson, R., Barton, C., Boehme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T. & Savage, S. (2012). *Measuring the cost of cybercrime*. URL: http://weis2012.econinfosec.org/papers/ Anderson_WEIS2012.pdf (accessed: 13.12.2016).

Arquilla, J. (1999). *Ethics and Information Warfare. In Strategic Appraisal: The Changing Role of Information in Warfare.* Ed. by Z. Khalilzad, J. White & A. Marsall. Santa Monica: RAND Corporation.

Bell, D. (1979). The Social Framework of the Information Society). In: *The Computer Age: A Twenty-Year View*. Ed. by M. L. Dertouzos & J. Moses. Cambridge, Mass.

Buzan, B., Wæver O. & et al. (1998). *Security: A new framework for Analysis.* Boulder: Lynne Rienner Publishers.

Chobanyan, V. A., & Shahalami, I. Y. (2013). Analysis and synthesis of the requirements for safety systems of objects of critical information infrastructure. *Issues of cybersecurity*. 1 (1), 17—27.

Denning, D. (2000). *Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services.* US House of Representatives. URL: http://www.stealth=ss.com/documents/pdf/CYBERTERRORISM.pdf (accessed: 04/20/14).

For a discussion of the military revolution that emerged between the two world wars. (1996). In: *Military Innovation in the Interwar Period*. Ed. by W. Murray & A. R. Millett. Cambridge: Cambridge University Press.

Freedman, L. (1998). International Security: Changing Targets. *Foreign Policy*, 110, 48—63.

Matveev, B. (2013). Status and prospects of development of national information security industry in 2014. *Cybersecurity*, 1(1), 61—64.

Metz, S., & Kievit, J. (1995). *Strategy and the Revolution in Military Affairs: From Theory to the Police.* Strategic Studies Institute. URL: http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?PubID=236 (accessed: 04.27.14).

Rosenzweig, P. (2010). The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence. *Deterring Cyberattacks: Informing Strategies and Developing Options*. National Research Council, 245—269.

Robinson, N., Disley, E., Potoglou, D., Reding, A., May Culley, D., Penny, M., Botterman, M., Carpenter, G., Blackman, C. & Millard, J. (2012). *Feasibility study fora European cyber crime centre*. Santa Monica, CA: RAND Corporation.

Sheehan, M. (2005). *International Security: and Analytical Survey*. London: Lynne Rienner Publishers.

Singer, P. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford University Press.

Weiss, G. W. (1996). The Farewell Dossier: Duping the Soviets. *CIA Studies in Intelligence*. URL: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm (accessed: 13.09.2016).

Received: 14.03.2017

For citations: Tsakanyan, V.T. (2017). The role of cybersecurity in world politics. *Vestnik RUDN. International Relations*, 17(2), 339—348.

About the author: *Tsakanyan Vladimir Tigranovich* — postgraduate student of the Department of Theory and History of International Relations of the RUDN University (e-mail: vladt20@mail.ru).

DOI: 10.22363/2313-0660-2017-17-2-339-348

РОЛЬ КИБЕРБЕЗОПАСНОСТИ В МИРОВОЙ ПОЛИТИКЕ

В.Т. Цаканян

Российский университет дружбы народов, Москва, Россия

Целью данной работы является оценка возрастающей роли кибербезопасности в мировой политике. В рамках этого исследования анализируются подходы к решению проблем кибербезопасности в Российской Федерации, США и КНР. Угрозы в этой области являются одними из основных для национальной и общественной безопасности, а также экономики, с которыми сталкивается государство в XXI в. Киберпространство является одной из определяющих черт современной жизни, которое сопряжено с рядом вопросов личной, национальной и международной безопасности. Существование многочисленных проблем в этой области, естественно, усиливает заинтересованность в их решении с точки зрения мировой политики, а потребность в обеспечении безопасности в киберпространстве становится все более актуальной, независимо от уровня.

Автор в своем исследовании подчеркивает, что в мире на данный момент превалирует два основных подхода к определению кибербезопасности. В рамках первого — кибербезопасность рассматривается в качестве инструмента реализации национальных интересов, это подтверждается тем, что основная часть современных теорий в этой области фокусируется на проблеме материальной выгоды. Второй подход, по мнению автора, заключается в том, что кибербезопасность не что иное, как инструмент оказания влияния на контрпартнеров в основном с помощью кибератак.

Автор делает заключение, что вопрос обеспечения кибербезопасности является довольно актуальной проблемой на сегодняшний день в мировой политике и заслуживает отдельного рассмотрения.

Ключевые слова: кибербезопасность, информационная безопасность, национальная безопасность, мировая политика, Соединенные Штаты Америки, Российская Федерация, Китайская Народная Республика, ООН

Дата поступления статьи: 14.03.2017

Для цитирования: *Цаканян В.Т.* Роль кибербезопасности в мировой политике // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2017. Т. 17. № 2. С. 339—348.

Сведения об авторе: *Цаканян Владимир Тигранович* — аспирант кафедры теории и истории международных отношений Российского университета дружбы народов (e-mail: vladt20@mail.ru).