DOI: 10.5817/MUJLT2017-1-7

WHAT IS AN INTERNATIONAL CYBERSECURITY REGIME AND HOW WE CAN ACHIEVE IT?

by

ILONA STADNIK*

This article explores the two mainstream directions of debates about the possibility of establishing a kind of international cybersecurity regime. It develops the idea of different governance models based on sovereignty, on the one hand, and multistakeholderism on the other. The application of international relations theory helps to understand the current process and stalemate initiatives regarding state cooperation in this field. In addition, the author pays attention to the applicability of the constructivism framework to the understanding of cybersecurity threats and the elaboration of international norms applicable to cyberspace. Finally, the article concludes with the idea that the multistakeholder approach to norm-making may become a viable solution to the problem of constructing an international cybersecurity regime.

KEY WORDS

Cybersecurity, Information Security, Sovereignty, Multistakeholderism, Regimes, Constructivism, Securitization

1. INTRODUCTION

Security is a key concern for all states. In fact, many of today's technologies are a direct result of research and development in national defense industries. However, at times technological advancements in other fields impinge on states' security concerns. The revolution in Information and Communications Technologies (ICT) presents one such case. With the emergence of global cyberspace at the beginning of the 21st

* ilona.st94@gmail.com, Saint-Petersburg State University, School of International Relations, Russia.

century, national cybersecurity has raised its priority in foreign and domestic policies of states. Since there is no international regime governing cyberspace, like the regime of high seas or outer space, states have been increasingly finding themselves in conflict over the breach of cyberspace that they perceive as a threat to their national security.

Cyberspace has gained a great importance for human interactions as well as for a higher level – international relations. More importantly, the cyber domain is multi-faceted – the flow of information and actions runs between these two quite separate (in comparison with other domains) levels. It may become necessary to regulate cyberspace as outer space, sea and airspace to establish common "*rules of game*" and to avoid arbitrary and potentially harmful actions of states. Bilateral agreements between nations, sometimes called as "*cyberpacts*", have become a widespread practice of strategic defense and cooperation.[1] As we are witnessing a dangerous trend of cyberspace militarization, some experts argue that wars of future are cyberwars.[2] This statement falls in the discourse of war as

> "*not merely a political act, but also a real political instrument, a continuation of political commerce, a carrying out of the same by other means.*"[3]

A war is an act of violence, aimed at making the adversary to compel to someone's will. Clauzewitz argued that war among nation states always stemmed from political reasons. Violence used for waging wars tended to exploit new discoveries in science and technology to counteract adverse violence. Connecting this idea to cyberspace seems to be logical, however

---

[1] See for example: U.S. Department of Homeland Security. (2011) *United States and India Sign Cybersecurity Agreement.* [press release], 19 July. Available from: https://www.hsdl.org/?view&did=682137 [Accessed 25 March 2015]; *Soglashenie mezhdu Pravitel'stvom Rossijskoj Federacii i Pravitel'stvom Kitajskoj Narodnoj Respubliki o sotrudnichestve v oblasti obespechenija mezhdunarodnoj informacionnoj bezopasnosti*, 8 May 2015. Available from: http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf [Accessed 10 June 2015]; *UK Government. (2015). UK-China Joint Statement on building a global comprehensive strategic partnership for the 21st Century.* [press release], 22 October. Available from: https://www.gov.uk/government/news/uk-china-joint-statement-2015 [Accessed 25 March 2015]; White House. (2015). *President Obama and President X joint statement on cybersecurity.* [press release], 25 September. Available from: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states [Accessed 25 March 2015].

[2] Clarke, R., Knake, R. (2010) *Cyber War: the Next Threat to National Security and What to Do about It.* New York: Harper Collins Publishers.

[3] Clausewitz, C; Howard, M., Editor and translator; Paret, P., Editor and translator (1989) [1832]. *On War*. Princeton, NJ: Princeton University Press.

there are a plenty of cyberskeptics who refuse to name future wars as cyberwars, because cyber attacks and computer operations may have only indirect potential for being physically violent, notwithstanding that they are kinds of classical hostile activities like espionage and sabotage.[4]

Militarization of cyberspace is a controversial and difficult for measuring process. The indirect indicators of militarization are instant messages from the media about an increase in expenses and development of military capabilities for cyberspace in different countries. Such capabilities include cyber offence and defense tools, involvement of IT specialists and programmers in defense strategies, creation of military units and commands responsible for cyberspace operations. In order to prevent the worst scenario and regulate the still unseen cyber arms race, there is a necessity to put much attention to the cyber dimension of international security.

The lack of a shared definition of what cyberspace and cybersecurity across the world is has led to a relatively slow negotiation process for the formation of an international cyberspace regime. The central theme of the contemporary debates is a future configuration of such an international regime. All parties involved in the issue can be roughly divided into two camps – adherents of the multistakeholder model (with equal participation of states, business and society in cyber governance issues) and supporters of the sovereignty-based model (with total government control over cyber infrastructure and information flows for security needs). This article focuses on analysis of ideas expressed by Russia, China, and the US in connection to possible cyber governance models, as these countries try to take the lead and put forward initiatives to the international community to promote their views and advance their interests. One of the factors that hampers inter-state dialog is the difference in interpretation of cybersecurity. On the one hand, it is about security of physical infrastructure – wired, fiber optic networks, routing equipment, storage systems and database servers; on the other, it may also encompass the security of information flows that circulate through this infrastructure. The last interpretation has direct implications for freedom of expression and access to information. These assumptions predominantly define

[4] See for example: Rid, T. (2013) *Cyber War Will Not Take Place*. New York: Oxford University Press.; Gartzke, E. (2013) the Myth of Cyber War. Bringing War in Cyberspace Back Down to Earth. *International Security*, Vol. 38, No. 2, pp. 41-73.

the features that underlie the governance models for the cyber domain and the participation of various stakeholders in particular.

2. GOVERNANCE MODELS

Very often scholars draw analogies between the cyber domain and the old domains of power such as the high seas, outer space or Antarctica because it is a *"global commons"*. The *"commons"* refers to resources that are not excludable but rival in consumption. However, the *"technical"* status of cyberspace that allowed for naming it *"commons"* is not a defining feature for such a comparison. Instead, from a legal perspective, the most important unifying feature of these domains is that they are not currently partitioned and governed according to traditional Westphalian sovereignty – in other words,

> *"states enshrined the non-sovereign status of old domains in international treaties"*.[5]

That is why we can single out some useful patterns for prospective global governance of cyberspace. Nevertheless, the analogy between cyber and old domains has its limits. The governance solutions were similar for the old domains — multilateral governance, governance by treaty, and certain demilitarization. But the cyber domain has distinct presets to be considered in the new governance model. These presets imply empowerment of private parties, governance through norms, and regulated militarization. The physical infrastructure level of cyberspace is located within national borders of states and often owned by private parties.[6] This fact prevents the usage of complete analogy between cyberspace and global commons.

According to Kristen Eichensehr, cyberspace has gone through several stages of cyber governance and its relations with sovereignty.[7] Since

---

[5] Eichensehr, K. (2015) The Cyber-Law of Nations. *Georgetown Law Journal*, 317. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447683 [Accessed 7 December 2016].

[6] According to Youchai Benkler (2000), information environment is composed of three layers - *"the physical infrastructure layer,"* the *"logical infrastructure layer,"* and *"the content layer."* the physical layer includes infrastructure like cables, wires, and routers. The logical layer consists of software. Above both is the content layer, which includes *"the stuff that gets said or written within any given system of communication"*. For the purposes of this article we consider cyberspace as a close concept to information environment.

[7] Eichensehr, K. (2015) The Cyber-Law of Nations. *Georgetown Law Journal*, 317. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447683 [Accessed 7 December 2016].

the 1990s, cyber itself was seen as sovereign – users, not governments, designed rules of the Internet because cyberspace

"needs and can create its own law and legal institutions".[8]

An example of such self-governance is the domain name system (DNS), which evolved from decisions made by engineers and the practices of Internet service providers. The second stage began in the early 2000s, when states started to realize the potential of the Internet as well as challenges it brought along. It has become clear that a new regulation is needed to facilitate the use of the Internet and prevent crimes related to the abuse of the ICT. In addition, an idea emerged that states could regulate the Internet by controlling its underlying hardware within their national borders. However, two issues define the feasibility of control: whether such a control is important for a state in order to protect its political stability; whether costs of imposing such a control are worthy.[9] Finally, the 2010s are characterized by government-to-government debates over cyber governance, the agenda being much more comprehensive than transnational cybercrime issues.

The current debate among states turns upon a particular model for global cybersecurity. As mentioned in the introduction, the alternatives are sovereignty-based and multistakeholder models. To develop this idea further by applying terms from international law we can add important extensions to both models. Thus, cyberspace can be treated, on the one hand, as a sovereign territory, and as a global commons on the other. Each extreme option implies a particular type of a legal regime. Also, even where the concept of territorial sovereignty cannot be applied to the full extent (as is the case in cyberspace), global governance is still possible – an international regime for the high seas and outer space are the examples. Another important question that is open for cyberspace but resolved in aforementioned examples is the role of private parties in governance (see Tab.1).[10]

---

[8] Johnson, D., Post, D. (1996) Law and Borders—The Rise of Law in Cyberspace, *Stanford Law Review*, 48, Available from: https://cyber.harvard.edu/is02/readings/johnson-post.html [Accessed 12 March 2015].

[9] Goldsmith, J. (1998) *The Internet and the Abiding Significance of Territorial Sovereignty, Indiana Journal of Global Legal Studies*, 5, Issue 2. Available from: http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1130&context=ijgls [Accessed 15 March 2015].

[10] The compilation is based on Eichensehr, K. (2015) the Cyber-Law of Nations. *Georgetown Law Journal*, 317.

	High Seas	Outer Space	Antarctic	Cyberspace*			
				USA	Russia	China	"Third option"
Governance by	Multilateral treaty	Multilateral treaty	Multilateral treaty	Globally accepted norms	Multilateral treaty	Multilateral treaty	Globally accepted norms
Participation of private parties	NO	NO	NO	YES	NO	NO	YES
Regulation of military activity	Limitation to peaceful purposes	Restricted militarization Peaceful activity on celestial bodies	Demilitarized zone	Regulated militarization	Demilitarization	Limitation to peaceful purposes	Regulated militarization

Tab. 1: Visions of governance models

Any governance model is defined by two main factors – who participate in decision-making and who has an overall control over taking and implementing decisions. As it can be seen from the table above, the US, Russia, and China support different solutions for cyberspace. Russia and China endorse a multilateral model in which states interact with each other and make decisions about policy and permissible actions in the cyber domain. The state-based model opens the door to a greater regulation of information. This is the focus of the proposed "*Cyber Code of Conduct*" by members of the Shanghai Cooperation Organization.[11] The United States and its allies endorse a multistakeholder model where Internet governance includes "*all appropriate stakeholders*", such as a private sector, civil society, academia, and individuals, in addition to governments.[12] The application of the multistakeholder model excludes the existence of any international treaty by definition. However, the need to define the "*rules of the game*" requires elaboration of globally accepted norms. Finally, the "*third option*" represents pure private governance, which is close to the idea of cyber as sovereign described by J. Barlow in his declaration of independence of cyberspace.[13] This idea has roots in the history of Internet commercialization and its deployment in some countries without close

[11] United Nations General Assembly. (2011) *Letter dated 12 September 2011 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations. A/66/359*. New York. Available from: http://undocs.org/A/66/359 [Accessed 15 March 2015]; United Nations General Assembly. (2015) *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations. A/69/723*. New York. Available from: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf [Accessed 15 March 2015].

[12] The White House. (2011) *The U.S. International Strategy for Cyberspace.* Washington D.C. Available from: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Accessed 15 March 2015].

government attention at initial stages. It led to the prevalence of private parties or professional IT communities in the first stage of the *"rules-creation"* process. However, the recent increased involvement of governments in regulation and examples of *"Internet takeovers"* in authoritarian states do not allow for speaking about the viability of this governance option.

The multistakeholder approach deserves describing in more detail. The very notion of multistakeholderism is new to the international relations theory and is undergoing theorization. M. Raymond and L. DeNardis define multistakeholderism

> *"as two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature, and characterized by polyarchic authority relations constituted by procedural rules."*[14]

By polyarchy they understand distribution of authority among a number of actors. Nevertheless, the distribution of authority is nominal in practice. The typology of stakeholder participation proposed by W. Drake reveals the level of involvement and, respectively, the distribution of authority. He distinguishes three types:[15]

- weak participation of non-state actors in government-led initiatives, limited ability to articulate their own position (as observers)
- limited capacity for participation in comparison with government representatives (as consulting experts in working groups)
- non-state actors act as equal peers with governments in the drawing up of the agenda, elaboration of rules, iterative consultations (*"strong multistakeholderism"*)

Obviously, the last ideal type can hardly be found in practice,[16] and there are plenty of reasons for that. Firstly, inadequate participation of non-state

---

[13] Barlow, J. Electronic Frontier Foundation. (1996) *A Declaration of the Independence of Cyberspace*. [record] 8 February, Davos. Available from: https://www.eff.org/cyberspace-independence [Accessed 15 March 2015].

[14] Raymond, M., DeNardis, L. (2015) *Multistakeholderism: anatomy of an inchoate global institution*. International Theory,7, Issue 3 November, pp. 572-616. Available from: https://doi.org/10.1017/S1752971915000081 [Accessed 3 July 2016].

[15] Drake, W. (2011) Multistakeholderism: Internal Limitations and External Limits. In: Wolfgang Kleinwächter (ed.) *Discussion Paper Series No. 1, MIND #2 Internet Policy Making*. Berlin-Nairobi: Internet and Society Collaboratory.

stakeholders is sometimes caused by lack of resources to travel and participate on-site. W. Drake emphasizes the reluctance of industrial democracies to invest in multistakeholder initiatives in order to facilitate organizational expenses and travel support, together with unwillingness to provide political support. Also, there is a gap in nominal and effective participation due to the character of the multistakeholder process, which is very complex in terms of procedures and amounts of information and the number of issues that stakeholders are supposed to discuss. Despite the idea of comprehensive inclusion of all concerned parties, multistakeholderism is not cooperative for newcomers because the workflow is dispersed among the communities, making it difficult to see the connections to the global aim of the whole process. Ultimately, C. Trautmann puts forward the idea of strengthening multistakeholderism positions by connecting

> *"multistakeholder fora with traditional decision-making bodies: the latter's task would be to implement the principles crafted in the former."*[17]

In this connotation, multistakeholderism seems to be rather a mode of "*decision-shaping*" than alternative decision-making.

3. GOVERNANCE MODELS

Turning back to the main question of the article – what is a cybersecurity regime? – we should explain what we understand under this notion. Regimes define the range of permissible actions by outlining explicit injunctions for actors. The most widely used definition of an international regime formulated by S. Krasner signifies that international regimes are

> *"implicit or explicit principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations."*[18]

---

[16] The IANA transition process may be acknowledged as illustration of strong multistakeholderism due to the ICANN policy of inclusion of governments, tech, business, and civil society in shaping the future of Internet governance.

[17] Trautmann, C. (2011) Multistakeholderism needs fundamental and decisive legitimation. In: Wolfgang Kleinwächter (ed.) *Discussion Paper Series No. 1, MIND #2 Internet Policy Making*. Berlin-Nairobi: Internet and Society Collaboratory.

[18] Krasner, S. (1982) Structural Causes and Regime Consequences: Regimes as Intervening Variables. *International Organization*, 2, Issue 36, Spring, pp. 185-205.

However, this definition is too broad; as J. Mearsheimer points out, such a formulation of a concept covers

> *"almost every regularized pattern of activity between states, from war to tariff."*[19]

A more restricted definition treats regimes as multilateral agreements among states, which aim to regulate national actions within an issue-area.[20] Nevertheless, both definitions deserve our attention in equal terms. Current controversy and uncertainty for the international regime for cyberspace lies within a particular type of regime – norms, rules, and procedures that guide actors' behavior, or a more restricted multilateral treaty with fixed penalties for disobedience. Here we can draw parallels with governance models described in the previous part. The former is softer and makes sense for the multistakeholder approach, while the latter resembles sovereignty-based governance.

Since an international regime can be also viewed as a form of cooperation and coordination between actors, it is worth considering how the main IR paradigms depict coordination and cooperation in cyberspace.

Realists considered cooperation problems as essential to the international system because of their anarchic structure.[21] The security dilemma is one of the examples of the cooperation problem. A security dilemma means a situation where efforts of one nation to improve its security decrease the security of others. In response, another nation tries to enhance its own defense capabilities. Such consecutive steps result in an arms race, worsening of diplomatic relations, and even in an open conflict. For cyberspace, it can unfold in the form of a cyber arms race. Countries try to build up their offensive cyber capabilities as, for example, espionage through intrusion to computer networks and dissemination of malware for spying purposes.[22] Another important factor that hampers cooperation is a difficulty in distinguishing between offensive

---

[19] Mearsheimer, J. (1995) The False Promise of International Institutions. *International Security*, 19, Issue 3, Winter, pp. 5-49.

[20] Haggard, S., Simmons, B. (1987) Theories of international regimes. *International Organization*, 41, Issue 3, pp. 491- 517.

[21] Waltz, K. (1979) Theory of international politics. Reading, MA: AddisonWesley Pub. Co.

[22] Craig, A., Valeriano, B. (2016) Conceptualising Cyber Arms Races. In: N. Pissanidis, H. Rõigas, M. Veenendaal (Eds.) *8th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications.

and defensive weapons and policies of states. If we focus on "*cybersecurity dilemma*", the definition can be transferred with particular details. In this case, it means that efforts by one country to enhance the security of its cyber infrastructure decrease the cybersecurity of others. Cybersecurity can be achieved either through the development of offensive or defensive cyber warfare capabilities. An important addition is that cyber-attack is easier, faster, and cheaper than cyber-defense, because

> "*effective defense must be successful against all attacks, whereas an attacker needs to succeed only once.*"[23]

In other words, factors of time for envision of coming attack as well as physical buffer space to resist it (features of conventional kinetic warfare) do not work in cyberspace, thus making offense capabilities a priority. Moreover, the "*cybersecurity dilemma*" is also complicated by problems of definition (what constitutes a cyber weapon) and attribution (the source of an attack).

Thus, cooperation between states on cybersecurity depends on whether offensive and defensive cyber warfare weapons and policies can be distinguished one from another. Even if countries agreed on the definition of cyber weapon, it would be highly difficult to distinguish between offensive and defensive cyber capabilities. The majority of military unites, in the USA and China in particular, responsible for cybersecurity, possesses both offensive and defensive capabilities. Such capabilities may include technologies of dual use. Solutions for cooperation proposed by realists include a cyber arms control in the form of a treaty, but the definition and attribution problems together with the "*verifiability problem*" (compliance to the treaty) make it a difficult task. In other words, it is hard to imagine the emergence of an IAEA-like (International Atomic Energy Agency) organization for cyberspace as it was organized to control nuclear energy use.

Liberal theories put an emphasis on cheating and dividing gains among states for cooperation and coordination problems.[24] For example, coordination problems in technocratic areas of global governance are solved

---

[23] National Research Council, Computer Science and Telecommunications Board. (1999) *Realizing the Potential of C4I: Fundamental Challenges*. Washington, D.C.: National Academy Press.

[24] Snidal, D. (1985) The limits of hegemonic stability theory. *International Organization*, 39, Issue 4, pp. 579-614.

through the creation of specialized international organizations. For instance – the International Telegraph Union created in 1865 and later the International Telecommunications Union (ITU) for allocation of global radio spectrum and satellite orbits, development of technical standards for interconnectedness and setting International Telecommunication Regulations (ITRs). The revision of ITRs in 2012 turned a coordination problem into a cooperation one because a part of the member states refused to sign the new ITRs, considering that they imposed more governmental control over the Internet.[25] Some countries (Russia, China) advocate giving the ITU responsibilities to define policy for Internet governance that is currently distributed among different entities of private and non-commercial background.[26] Governance of distribution of Internet names and numbers together with the development of technical protocols can be firmly classified as an issue of low politics and involve coordination problems. But in recent years it was highly politicized and brought together with security concerns that the agreement on a particular equilibrium of governance model presents difficult negotiation problems.[27]

Liberalist thinkers argued that international institutions (including international rules, norms, principles, and decision-making procedures) can help to facilitate cooperation even in the face of a security dilemma.[28] International norms can play roles in both constraining state behavior and encouraging interstate cooperation. In the context of the IR theory, norms refer to

> *"collective understandings of the proper behavior of actors"*.[29]

---

[25] International Telecommunications Union. (2012) *WCIT-12 Final Acts*. Dubai. Available from: www.itu.int/en/wcit-12/documents/final-acts-wcit-12.pdf [Accessed 19 April 2015].

[26] Kurbaljia, J. (2014) *Introduction to Internet governance.* 6th ed. Malta: DiploFoundation.

[27] ICANN is undergoing the process of its reorganizations towards more accountability and independence. Transition of the US National Telecommunications and Information Administration (NTIA) oversight role over IANA came to an end. It started in March 2014, and two years later a final proposal (elaborated upon with participation of all stakeholders) was introduced to the NTIA for consideration. The summer of 2016 was named the *"end of the era of American control over the Internet"*.

[28] See for example: Keohane, R. (1984) *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press; Krasner, S. (1983) *International Regimes*. Ithaca: Cornell University Press; Axelrod, R. Keohane, R. (1986) *Cooperation Under Anarchy*. Princeton: Princeton University Press; Martin, L., Simmons, B. (1998) Theories and Empirical Studies of International Institutions. *International Organization*, 52, Issue 4, Autumn, pp. 729-757.

[29] Legro, J. (1997) Which Norms Matter? Revisiting the 'Failure' of Internationalism. *International Organization*, 51, Issue 1.

Although norms are not always codified in law, they often inspire or lead to the development of international law. Institutions can help create and foster norms, although norms can also develop at the domestic level and then "*diffuse*" throughout the international system.[30] As institutions serve as instruments through which states can achieve cooperation, they may impose constraints on a state behavior. But these constraints are usually accepted as the inevitable costs of cooperation.

Thus "*cybersecurity dilemma*" may potentially be resolved through the creation of international institutions. Moreover, liberalism acknowledges non-state entities as actors, so a possible international organization for maintenance of cybersecurity can be composed of states and non-state actors (represented by the IT industry, for example). Such option would enable participants to strengthen trust by revealing capabilities and methods to identify cyber war incidents and share defensive technologies. The IT industry can greatly contribute its expertise to foster trust and transparency. On the other hand, participation in such an organization will require members to share sensitive information about their cyber capabilities, which they are not willing to do, fearing it could weaken their relative positions. Simultaneously, cyber powers (like the US, for instance) would hardly be ready to join such an organization in an attempt to avoid any accountability for their offensive cyber capabilities and to keep their relative dominance in the cyber domain.

The constructivist approach pays attention to the perception of reality that defines the reason for cooperation between states on security issues. Although many constructivists do not contest the idea that there is a material basis to security threats, they argue that the labeling of diverse activities as threats to national security is a product of "*intersubjective interpretation*".[31] Hence, discursive practices of cyber threats formulation and perception play an important role.

Cybersecurity discourse is about more than one threat form, ranging from computer viruses and other malicious software to the cyber-crime activity and the categories of cyber-terror and cyber-war. Each sub-issue is

---

[30] Finnemore, M., Sikkink, K. (1998) International Norm Dynamics and Political Change. *International Organization*, 52, Issue 4.

[31] See for example: Dartnell, M. (2003) Weapons of Mass Instruction: Web Activism and the Transformation of Global Security. Millennium, 32, Issue 3, pp. 477-499; Hansen, L., Nissenbaum, H. (2009) Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53, Issue 4, pp. 1155-1575.

represented and treated differently in the political process and at different points in time.[32] That is why the theory of securitization introduced by Buzan, Weaver and De Wilde can be useful to draw the link between a national security and cyber domain.[33]

> *"The question of when a threat becomes a national security threat depends on what type of threat it is, how the recipient perceives it."*[34]

Securitization is a process of justifying a new security policy in several steps. Firstly, an actor (it can be a government or secondary actors) starts to voice serious concerns over a topic and formulates threats to a referent object (a nation, a state) that has to be protected. The second step is audience validation of a formulated threat as an existential threat. When the necessity is acknowledged, an actor starts to design required policies and actions needed to be taken to ensure security of the referent object. For constructivist studies, the scale of analysis matters a lot – actors and referent objects comprise a unique set of threats. Thus, securitization theory can help to trace back states' intentions by analyzing the language of the cybersecurity discourse. Moreover, the very word *"cybersecurity"* is replaced sometimes (or even disappears from the public discourse) by information security. Consequently, threat representations differ in a substantial way. Information security implies more sensitive issues for national security – threats acquire a psychological and ideological context – for instance, dissemination of harmful information that can destroy political stability and public order. The cyber/information security discourse differs a lot in Russia, China, and the US.[35]

The analysis of threat perceptions in Russia, China, and the US reveals common grounds in cyber threat perceptions for further cooperation

---

[32] Dunn Cavelty, M. (2013) From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review,* 15, Issue 1, March.

[33] Buzan, B., Waever, O. and De Wilde, J. (1998). *Security: a New Framework for Analysis*. Boulder, CO: Lynne Rienner.

[34] Buzan, B. (1991). *Peoples, States and Fear: an Agenda for International Security Studies in the Post-Cold War Era*, 2nd ed. Boulder, CO: Lynne Rienner.

[35] The Russian Government. (2016) *Doktrina Informacionnoi Bezoasnosti*. 5 December, Moscow. Available from: http://kremlin.ru/acts/bank/41460. [Accessed 10 February 2017]; the White House. (2011) the *U.S. International Strategy for Cyberspace*. Washington D.C. Available from: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Accessed 10 February 2017]; Chang, A. (2014) *Warring State: China's Cybersecurity Strategy*. [online] 3 December, Center for a New American Security. Available from: https://www.cnas.org/publications/reports/warring-state-chinas-cybersecurity-strategy [Accessed 10 February 2017].

to mitigate the negative effect for a national security (see Tab.2).[36] Colored boxes indicate what threat or contentious issue is under the country's focus. The last row of the table emphasizes possible policy areas for global cooperation for the norm-making process.

Threats and contentious issues		ICT use in violation of international law – territorial integrity and sovereignty	Militarization of cyberspace	Political cyber espionage	ICT use in terrorist purposes	Cybercrime (network exploitation, intrusion, e.g. crimes with ICT use)	Dissemination of information harmful for public order and society (including extremism)	Digital gap and IT technology dependence from other country	Information expansion of foreign media in country and distortion of domestic and international news picture	Threats to safe and stable functioning of the global and national critical information infrastructures	Cyber attacks on national critical infrastructure and industrial control systems	Intellectual property theft (industrial cyber espionage)	Threats to Internet freedom and free flow of information	
Common grounds	USA													USA
	China													China
	Russia													Russia
Instruments for cooperation					To be defined	Mechanisms of investigation and law enforcement + Budapest convention revision				Internet Governance	Confidence Building Measures			

Tab. 2: Common grounds for cooperation in combating cyber threats

Russia and China are closer to each other in threat perceptions. More importantly, they put an emphasis on sovereignty in cyberspace, while the US is concerned with network security and a free flow of information for economic and political reasons. However, there are issues that all three countries acknowledge as dangerous for a national security – ICT use for terrorist purposes, cybercrime, threats to safe and stable functioning of the global and national critical information infrastructures, and cyberattacks on the national critical infrastructure and industrial control systems. As cyberspace and the Internet are a transnational and single world domain (at least so far, keeping in mind the tendencies for Internet fragmentation), there is a need to elaborate global norms of behavior (applicable for non-state actors also) with national enforcement. The first steps are already taken for outlined issues: confidence-building

[36] Based on content analysis of national strategic documents. The complete list is introduced in references in the end of the article.

measures in cyberspace;[37] the Budapest convention to combat cybercrime;[38] Internet governance evolution; and the reform of ICANN. Yet, all stakeholders are still at odds with these issues.

4. CONSTRUCTIVISM FOR NORM-MAKING

In addition, the constructivist approach also can shed light on the norm-creation process. Constructivists have done a great deal of work attempting to explain the emergence of new international norms. The theory of strategic social construction proposed by M. Finnemore and K. Sikkink can help to answer the question of how the cybersecurity regime can be achieved.[39] Their proposed *"life cycle"* of norms consists of norm emergence, norm cascade, and internalization. Firstly, a norm emerges from the need for desirable behavior of stakeholders, but it never *"enters a normative vacuum"* and has to compete with other interests. Importantly, international organizations serve as a platform through which norms can be promoted, due to their expertise. We will develop the example of such norms' promotion for cyberspace later in this paragraph. Moreover, institutionalization of specific rules and principles through such organizations helps to clarify what constitutes the norm and its violation. Further steps involve consecutive adoption of newly created norm by states, in other words, *"norm cascade"*. Finnemore and Sikkink argue it happens because states want to maintain their identity of an international community member, thus showing conformity. Ultimately, *"automatic conformance with the norm"* is internalization – an extreme form of the norm cascade.

At the same time, a normative change may become the result of procedural changes that lead to the creation of new policies. Social practices and background knowledge are central notions for understanding. E. Adler and V. Pouliot define practices as

---

[37] OSCE. (2016). Permanent Council Decision No. 1202. OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. Vienna. Available from: http://www.osce.org/pc/227281 [Accessed 10 February 2017].

[38] Signed by 50 countries. The United States signed and ratified this Convention in 2007. China did not sign the document, nor did Russia because of the problem "article 32(b)". This article 32 (b) of the Convention allows the obtaining, without the consent of the participating countries, access to the computer data stored on its territory, i.e., to conduct cross-border investigations and investigative activities. Russia considers such a provision a violation of sovereign rights of states.

[39] Finnemore, M., Sikkink, K. (1998) International Norm Dynamics and Political Change. *International Organization*, 52, Issue 4.

> *"socially meaningful patterns of action which, in being performed more or less competently, simultaneously embody, act out and possibly reify background knowledge and discourse in and on the material world."*[40]

This background knowledge is, in fact, procedural rules that condition the emergence of norms for social practices. If we narrow them to diplomatic practices, we will get written and unwritten rules that constitute the specific game of multilateral diplomacy as procedural rules.[41] for states engaged in the negotiation process, it is highly important to have the ability to use such procedural rules in their favor.

Another point for procedural rules focuses on their ability to facilitate negotiations on a sensitive issue. In our case, the agreement on norms of responsible state behavior for the use of ICTs presents a highly contentious cooperation problem. However, the UN Group of governmental experts on information security (UN GGE)[42] was able to achieve tangible results by the third round of negotiations because the participating states did not object to procedural rules of presenting their positions and assessing those of their counterparts. Thus, Russia and the US came to an agreement that International Law can be applied to the use of ICTs (it is worth noting that neither cyberspace nor information space is used in GGE reports for the satisfaction of the countries' positions). The Table below illustrates the results of the GGE work done by 20 countries on compiling the list of existing and emerging threats in the use of ICT.[43] It also illustrates the progress in alignment of countries' positions on the issue.

---

[40] Adler, E., Pouliot, V. (2011). International practices. *International*. Theory, 3, p. 136

[41] Adler-Nissen, R., Pouliot, V. (2014) Power in practice: Negotiating the international intervention in Libya. European Journal of International Relations, 20, Issue 4.

[42] United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UNODA. Russia, China, and the US were country-members for each GGE convocation.

[43] Table is based on: United Nations General Assembly. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174*. New York. Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement [Accessed 6 April 2016].

Threats and contentious issues		ICT use in violation of international law – territorial integrity and sovereignty	Militarization of cyberspace	Political cyber espionage	ICT use in terrorist purposes	Cybercrime (network exploitation, intrusion, e.g. crimes with ICT use)	Dissemination of information harmful for public order and society (including extremism)	Digital gap and IT technology dependence from other country	Information expansion of foreign media in country and distortion of domestic and international news picture	Threats to safe and stable functioning of the global and national critical information infrastructures	Cyber attacks on national critical infrastructure and industrial control systems	Intellectual property theft (industrial cyber espionage)	Threats to Internet freedom and free flow of information	
Common grounds	USA				■	■				■	■	■	■	USA
	China	■		■	■	■	■	■		■	■			China
	Russia	■	■	■	■	■	■	■	■	■	■			Russia
	GGE		▒		▒					▒	▒			GGE

Tab. 3: Finding common grounds within the UN GGE

Nevertheless, the GGE recommendations for norms, rules, and confidence building measures are still non-binding and serve rather as guidelines for voluntary observance than institutionalized norms with clear consequences for incompliance. One of the problems to turn these recommendations into legally binding rules is the complicated nature of cyberspace and a wide circle of stakeholders that includes not only governments but private actors as well. States are trying to solve a puzzle: even if they follow strategic social construction with procedural norms of UN General Assembly First Committee, what will the international regime for cyberspace look like? One way that is advocated by the US and its allies is to apply the existing international norms to cyberspace – those written in the UN Charter, the law of armed conflict and law of responsible state behavior. Partly, the GGE resulted in acknowledging such a way. On the other hand, cyber/information space may require a special multilateral treaty. The main challenge for this option is the definition of the space under consideration, whether it is global commons or a sovereign territory. Uncertainty in this issue blocks any further state cooperation.

K. Erskine and M. Carr define main challenges for developing norms for cyberspace.[44] First, they are new practices displaying the characteristics of cyber-governance of the global domain system, coordination of individual networks, social media usage, protection from cyberattacks,

[44] Erskine, K., Carr, M. (2016) Beyond 'Quasi-Norms': the Challenges and Potential of Engaging with Norms in Cyberspace. In: Anna-Maria Osula and Henry Roigas (Eds.) *International Cyber Norms: Legal, Policy & Industry Perspectives*. Tallinn: NATO CCD COE Publications.

and the like. There is still no clear understanding of what behavior is wrong or right that would be accepted by all stakeholders. Another factor is competing value systems of stakeholders – understanding of the privacy/ transparency/anonymity balance that defines the perception of security in cyberspace. As can be seen from Tab. 2, even the three countries differ in their preferences. In addition, a variety of stakeholders also contribute to the values competition. For example, private sector aims at maximizing its profits rather than at concerning with national security issues. Finally, the problem of attribution allows actors to deny any allegations for harmful activities in cyberspace.

In the end, Erskine and Carr stress the idea of quasi-norms for cyberspace. Stakeholders

> *"will seek to impose rules and codes of conduct on practices that further their interests or values"*;

but

> *"imposed rules are not norms, they are normative aspirations"*,

because norms should first of all be internalized by stakeholders, since norms inform the behavior through the prescriptive and evaluative nature.[45] In this respect, the normative aspiration of the US to import norms from the law of armed conflict to cyberspace may seem useless, as imported norms from another domain *"risk to significantly lose meaning and moral force"*.

5. CONCLUSIONS

The international cybersecurity regime is at the initial stages of its construction, a norm-creation stage. However, the contours of this regime are still vague. There are two possible scenarios for further development – adjustment of the existing international law to cyberspace peculiarities (which is likely to be a stalemate), or elaboration of special governance mechanisms. The special governance mechanisms remain mired in uncertainty, raising questions if cybersecurity is subject to top-down multilateral regulation, or more non-state stakeholders should have their say, including the IT industry.

---

[45] Ibid.

The multilateral approach for cybersecurity would hardly define the new regime. The reasons for such argument are strong: there is still no common agreement on the substance of a treaty or a convention on international cybersecurity. Cyberspace and information space differ substantially in their underlying meaning. The content analysis of the countries' perceived cyber/information threats revealed the fault line between the values promoted by the US, on the one hand, and Russia and China on the other. While the US is concerned with secure computer networks simultaneously providing the open, secure Internet with free flow of information and freedom of expression, it also builds up offensive cyber capabilities to protect the current status quo. Russia and China place high priority on information security and combating against threats that may harm society, the political regime, and the stability of a state. Such threats also include terrorism, extremism, and separatism; moreover, Russia emphasizes information expansion of the foreign media in the country and distortion of the domestic and international news picture.

Cybersecurity is a very complex multi-component issue for a single international regime. Despite divergence in threat perceptions, the three countries have common concerns: ICT use for terrorist purposes, cybercrime, stability and resiliency of the Internet critical infrastructure, network security, and militarization of cyberspace. The UN GGE work made a significant contribution to the consensus between member-states and even broadened the understanding of common challenges. But the group still has a long way to go for achieving tangible results. If to separately regulate each area, agreed to be a high priority for countries, multilateral approach will still be weak despite the assumption that the established procedural rules for norm-formulation make this process easier. That was proven by the example of the impossibility of the arms control treaty for cyberspace: there is still no globally accepted definition of what a cyber weapon is. In addition, technologies of dual-use are predominant in the IT area. Though states have already agreed on a number of international treaties for arms-control and non-proliferation, the pool of procedural rules and behavior patterns is widely used; the cyber arms control treaty is hard to design because of the difficulties in controlling compliance.

Confidence building measures (CBMs) to protect critical infrastructure could be taken through a multilateral approach – and there are already

examples of bilateral agreements, and even UN GGE recommendations contain a substantial list of particular steps for CBMs. In reality, the majority of cases show that CBMs exist only on paper. And here we can see a security dilemma – if one state exhibits more vulnerabilities than another, then the second state would probably use this information with malicious intentions.

The multilateral approach also has another considerable drawback – it neglects non-state actors in the process of norm-making. The case of cyberspace is unique in the sense that the IT industry exerts a great influence on the cyber policy both in creating security solutions and in constructing new cyber threats as collateral consequences of their business.

One of the areas for ensuring stability and resiliency of the Internet critical infrastructure is the Internet governance. It was multistakeholder from the very beginning. States entered *"the game"* after the distributed system of allocation and governance of Internet critical resources had been invented. Any attempts by states (Russian and China in particular) to establish control or intrude into the governance system are firmly pushed back. Undoubtedly, states will have a say in the Internet governance policy, but formulas for respective roles are still to be found.

Multistakeholderism should not be taken as a good solution to problems caused by cyberspace features. It has a lot of limitations, where the distribution of authority between stakeholders is the most strong. One of the problems for a multistakeholder approach to cybersecurity is to ensure a win-win public-private partnership. Firstly, the IT industry is willing to participate in security projects for national critical infrastructure when economic benefits overcome costs. Secondly, the absence of shared principles of cyber or information security that define the privacy/security equilibrium considerably hampers collaboration. Even in democratic countries, the IT industry suffers from the effects of the government policy aimed at protecting national interests and security to the detriment of protecting various human rights, such as privacy and free flow of information. At least, multistakeholderism may hopefully produce principles that would constitute the basis for cybersecurity norms to be accepted by all stakeholders.

LIST OF REFERENCES

[1] Adler, E., Pouliot, V. (2011). International practices. *International. Theory*, 3, p. 136.

[2] Adler-Nissen, R., Pouliot, V. (2014) Power in practice: Negotiating the international Intervention in Libya. *European Journal of International Relations*, 20, Issue 4.

[3] Axelrod, R. Keohane, R. (1986) *Cooperation Under Anarchy*. Princeton: Princeton University Press.

[4] Barlow, J. Electronic Frontier Foundation. (1996) *A Declaration of the ndependence of Cyberspace.* [record] 8 February, Davos. Available from: https://www.eff.org/cyberspace-independence [Accessed 15 March 2015].

[5] Buzan, B. (1991). *Peoples, States and Fear: an Agenda for International Security Studies in the Post-Cold War Era*, 2nd ed. Boulder, CO: Lynne Rienner.

[6] Buzan, B., Waever, O. and De Wilde, J. (1998). *Security: a New Framework for Analysis*. Boulder, CO: Lynne Rienner.

[7] Chang, A. (2014) *Warring State: China's Cybersecurity Strategy*. [online] 3 December, Center for a New American Security. Available from: https://www.cnas.org/publications/reports/warring-state-chinas-cybersecurity-strategy [Accessed 10 February 2017].

[8] Clarke, R., Knake, R. (2010) *Cyber War: the Next Threat to National Security and What to Do about It.* New York: HarperCollins Publishers.

[9] Clausewitz, C; Howard, M., Editor and translator; Paret, P., Editor and translator (1989) [1832]. *On War*. Princeton, NJ: Princeton University Press.

[10] Craig, A., Valeriano, B. (2016) Conceptualising Cyber Arms Races. In: N. Pissanidis, H.Rõigas, M.Veenendaal (Eds.) *8th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications.

[11] Dartnell, M. (2003) Weapons of Mass Instruction: Web Activism and the Transformation of Global Security. *Millennium*, 32, Issue 3, pp. 477-499.

[12] Drake, W. (2011) Multistakeholderism: Internal Limitations and External Limits. In: Wolfgang Kleinwächter (ed.) *Discussion Paper Series No. 1, MIND #2 Internet Policy Making*. Berlin-Nairobi: Internet and Society Co:llaboratory.

[13] Dunn Cavelty, M. (2013) From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, 15, Issue 1, March.

[14] Eichensehr, K. (2015) the Cyber-Law of Nations. *Georgetown Law Journal*, 317. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447683 [Accessed 7 December 2016].

[15] Erskine, K., Carr, M. (2016) Beyond 'Quasi-Norms': the Challenges and Potential of Engaging with Norms in Cyberspace. In: Anna-Maria Osula and Henry Roigas (Eds.) *International Cyber Norms: Legal, Policy & Industry Perspectives.* Tallinn: NATO CCD COE Publications.

[16] Finnemore, M., Sikkink, K. (1998) International Norm Dynamics and Political Change. *International Organization*, 52, Issue 4.

[17] Gartzke, E. (2013) The Myth of Cyber War. Bringing War in Cyberspace Back Down to Earth. *International Security*, Vol. 38, No. 2, pp. 41-73.

[18] Goldsmith, J. (1998) The Internet and the Abiding Significance of Territorial Sovereignty, *Indiana Journal of Global Legal Studies*, 5, Issue 2. Available from: http://www.repositorylaw.indiana.edu/cgi/viewcontent.cgi?article=1130&context=ijgls [Accessed 15 March 2015].

[19] Haggard, S., Simmons, B. (1987) Theories of international regimes. *International Organization*, 41, Issue 3, pp. 491- 517.

[20] Hansen, L., Nissenbaum, H. (2009) Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53, Issue 4, pp. 1155-1575.

[21] International Telecommunications Union. (2012) *WCIT-12 Final Acts*. Dubai. Available from: www.itu.int/en/wcit-12/documents/final-acts-wcit-12.pdf [Accessed 19 April 2015].

[22] Johnson, D., Post, D. (1996) Law and Borders — The Rise of Law in Cyberspace, *Stanford Law Review*, 48, Available from: https://cyber.harvard.edu/is02/readings/johnson-post.html [Accessed 12 March 2015].

[23] Keohane, R. (1984) *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.

[24] Krasner, S. (1982) Structural Causes and Regime Consequences: Regimes as Intervening Variables. *International Organization*, 2, Issue 36, Spring, pp. 185-205.

[25] Krasner, S. (1983) International Regimes. Ithaca: Cornell University Press.

[26] Kurbaljia, J. (2014) *Introduction to Internet governance.* 6th ed. Malta: DiploFoundation.

[27] Legro, J. (1997) Which Norms Matter? Revisiting the 'Failure' of Internationalism. *International Organization*, 51, Issue 1.

[28] Martin, L., Simmons, B. (1998) Theories and Empirical Studies of International Institutions. International *Organization*, 52, Issue 4, Autumn, pp. 729-757.

[29] Mearsheimer, J. (1995) The False Promise of International Institutions. *International Security*, 19, Issue 3, Winter, pp. 5-49.

[30] National Research Council, Computer Science and Telecommunications Board. (1999) *Realizing the Potential of C4I: Fundamental Challenges*. Washington, D.C.: National Academy Press.

[31] OSCE. (2016). *Permanent Council Decision No. 1202*. OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. Vienna. Available from: http://www.osce.org/pc/227281 [Accessed 10 February 2017].

[32] Raymond, M., DeNardis, L. (2015) Multistakeholderism: anatomy of an inchoate global institution. *International Theory*,7, Issue 3, November, pp. 572-616. Available from: https://doi.org/10.1017/S1752971915000081 [Accessed 3 July 2016].

[33] Rid, T. (2013) *Cyber War Will Not Take Place*. New York: Oxford University Press.

[34] Snidal, D. (1985) The limits of hegemonic stability theory. *International Organization*, 39, Issue 4, pp. 579-614.

[35] The Russian Government (2015) *Soglashenie mezhdu Pravitel'stvom Rossijskoj Federacii I Pravitel'stvom Kitajskoj Narodnoj Respubliki o sotrudnichestve v oblasti obespecheni a mezhdunarodnoj informacionnoj bezopasnosti*, Moscow. Available from: http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf [Accessed 10 June 2015].

[36] The Russian Government. (2016) *Doktrina Informacionnoi Bezoasnosti*. 5 December, Moscow. Available from: http://kremlin.ru/acts/bank/41460 [Accessed 10 February 2017].

[37] The White House. (2011) *The U.S. International Strategy for Cyberspace*. Washington D.C. Available from: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Accessed 15 March 2015].

[38] The White House. (2015). *President Obama and President X joint statement on cybersecurity* [press release], 25 September. Available from: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states [Accessed 25 March 2015].

[39] Trautmann, C. (2011) Multistakeholderism needs fundamental and decisive legitimation. In: Wolfgang Kleinwächter (ed.) *Discussion Paper Series No. 1, MIND #2 Internet Policy Making.* Berlin-Nairobi: Internet and Society Co:llaboratory.

[40] U.S. Department of Homeland Security. (2011) *United States and India Sign Cybersecurity Agreement*. [press release], 19 July. Available from: https://www.hsdl.org/?view&did=682137 [Accessed 25 March 2015].

[41] UK Government. (2015*). UK-China Joint Statement on building a global comprehensive strategic partnership for the 21st Century*. [press release], 22 October. Available from: https://www.gov.uk/government/news/uk-china-joint-statement-2015 [Accessed 25 March 2015].

[42] United Nations General Assembly. (2011) *Letter dated 12 September 2011 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations. A/66/359.* New York. Available from: http://undocs.org/A/66/359 [Accessed 15 March 2015].

[43] United Nations General Assembly. (2015) *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations. A/69/723*. New York. Available from: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf [Accessed 15 March 2015].

[44] United Nations General Assembly. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174*. New York. Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement [Accessed 6 April 2016].

[45] Waltz, K. (1979) Theory of international politics. Reading, MA: AddisonWesley Pub. Co.

LIST OF DOCUMENTS FOR TAB. 2 AND TAB. 3

[1] SCO. (2009) *Soglashenie mezhdu pravitelstvami gosudarstv – chlenov SHanhajskoj organizacii sotrudnichestva o sotrudnichestve v oblasti obespecheniya mezhdunarodnoj informacionnoj bezopasnosti*. Available from: http://docs.cntd.ru/document/902289626 [Accessed 25 March 2016].

[2] The Russian Council of Federation. (2013) *Koncepciya strategii kiberbezopasnosti*, Available from: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf [Accessed 25 March 2016].

[3] The Russian Ministry of Defense. (2011). *Konceptualnye vzglyady na deyatelnost vooruzhennyh sil Rossijskoj Federacii v informacionnom prostranstve.*

[4] The Russian Ministry of International Affairs. (2011). *Convetion on International Information Security.* Available from: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=en_GB [Accessed 25 March 2016].

[5] The Russian President. (2009) *O Strategii nacionalnoj bezopasnosti Rossijskoj Federacii do 2020 goda.* Available from: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102129631 [Accessed 25 March 2016].

[6] The Russian President. (2014) *Voennaya doktrina Rossijskoj Federacii.* Available from: http://kremlin.ru/events/president/news/47334 [Accessed 25 March 2016].

[7] The Russian President. (2015) *Strategiya nacionalnoj bezopasnosti Rossijskoj Federacii.* Available from: http://kremlin.ru/acts/news/51129 [Accessed 25 March 2016].

[8] The Russian President. (2015) *Voennaya doktrina Rossijskoj Federacii*. Available from: http://kremlin.ru/supplement/461 [Accessed 25 March 2016].

[9] The Russian President. (2016) *Doktrina Informacionnoi Bezopasnosti*. 5 December, Moscow. Available from: http://kremlin.ru/acts/bank/41460 [Accessed 10 February 2017].

[10] United Nations General Assembly. (2015) *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations. A/69/723.* New York. Available from: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf [Accessed 25 March 2016].

[11] The US Department of Defense (2015). *The DoD Cyber strategy*. Available from: https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [Accessed 25 March 2016].

[12] The US Department of Homeland Security. (2003) *The national strategy for secure cyberspace.* Available from: https://www.dhs.gov/national-strategy-secure-cyberspace [Accessed 25 March 2016].

[13] The US Department of Homeland Security. (2009) *Cyberspace policy review*. Available from: https://www.dhs.gov/publication/2009-cyberspace-policy-review [Accessed 25 March 2016].

[14] The US Senate. (2014) *Worldwide Threat Assessment of the US Intelligence Community. Testimony of J. Clapper*. 29 January, Washington. Available from: https://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf [Accessed 25 March 2016].

[15] The US Senate. (2015) *Worldwide Threat Assessment of the US Intelligence Community. Testimony of J. Clapper*. 26 February, Washington. Available from: https://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee [Accessed 25 March 2016].

[16] The White House (2010) *National Security Strategy*. Available from: http://nssarchive.us/national-security-strategy-2010/ [Accessed 25 March 2016].

[17] The White House. (2011) *The U.S. International Strategy for Cyberspace*. Washington D.C. Available from: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Accessed 25 March 2016].

[18] China's Central Military Commission (2014). *Opinion on Further Strengthening Military Information Security Work.*

[19] China's National Informatization Leading Group. (2006) *National Informatisation Development Strategy, 2006-2020.*

[20] China's State Informatization Leading Group. (2003) *Opinions for Strengthening Information Security Assurance Work ("Document 27").* Available from: http://www.btpta.gov.cn/publish/portal7/tab550/info92345.htm [Accessed 25 March 2016].

[21] The Information Office of the State Council. (2013) *White Paper: The Diversified Employment of China's Armed Forces*. Available from: http://www.nti.org/media/pdfs/China_Defense_White_Paper_2013.pdf [Accessed 25 March 2016].

[22] The Information Office of the State Council. (2015) *China's Military Strategy*. Available from: http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm [Accessed 25 March 2016].