THE RUSSIAN SEGMENT OF INTERNET AS A RESILIENT BATTLEFIELD

Juha KUKKOLA, M.Soc.Sci
Juha.kukkola@mil.fi
Department of Warfare
Finnish National Defence University, Helsinki, Finland

Abstract

After the public demonstrations of 2012-2013 and the souring of relations with the West because of the illegal annexation Crimea the Russian Federation has clamped down on Internet freedom. At first sight, this policy could be considered only as a reaction of an authoritarian regime to internal dissention and external propaganda. But after the publication of multiple government doctrines, programs and laws treating information security, and statements by political leadership implying that Russia is planning to disconnect its national segment of Internet it seems that something more is going on. This article claims that Russia is building a system-of-systems of cyber security and defence measures that it believes enables it to withstand cyber-attacks against its critical national assets. The subsystems of this entity have different functions and are controlled by various actors but can be joined to a centrally controlled system. This paper builds on previous research on Russian cyber strategy by aiming, firstly, to describe the developing national system-of-systems and, secondly, to analyse its effects on the resilience of the national segment of Internet during peace time, intensified competition, conflict and war. The paper argues that the Russian Federation is aiming for a flexible, although complex and possibly vulnerable, national cyber defence system that could ultimately provide it a decisive advantage in a state-to-state cyber conflict.

Keywords: Russia, cyber defence, national segment of Internet, system-of-systems, resilience.

Introduction

After the public demonstrations of 2012-2013 and the souring of relations with the West because of the illegal annexation Crimea the Russian Federation has clamped down on Internet freedom (Soldatov 2017; Freedom House 2017). Starting from 2014 the Russian Federation has issued laws limiting the freedom of Internet in the country. Consequently, it published Information Security Doctrine in 2016 which aimed to secure and control 'the national segment of Internet'. The next year the Russian government adopted the Strategy on the Development of an Information Society in the Russian Federation for 2017-2030 and the state program of 'Digital Economy' which among other things declared that Russia would achieve 'digital sovereignty' by 2020. In 2017-2018 the government published implementation plans on 'Digital Economy' which stated that the Russian state would duplicate the most critical services of its national segment of Internet and would ensure that by 2024 only 10% of the Russia's internal Internet traffic would go through foreign servers. Additionally, in 2017 Russia published a law on critical information infrastructure (CII) which aims to categorize national critical information infrastructure, obligates private owners to secure them and gives security services the mandate to monitor adherence to it. Moreover, Russia has been conducting state-level exercises to manage the disconnection of the national segment from the wider Internet from 2014.[1]

This article claims that what all these policies build up to is a system-of-systems[2] of cyber security and defence measures that Russia believes enables it to withstand cyber-attacks against its critical national assets. The project is a proof of the so-called fragmentation of Internet that has been going on for so time now. This fragmentation is drive by some states, mainly authoritarian, who strive to create physically, logically and semantically separated islands of Internet that can be controlled by the state (Demchak & Dombrowski 2013; DeNardis 2014; Mueller 2017). The states have their various reasons for doing this, but this paper argues based on previous research that, at least partially, Russia approaches this process from the point of

[1] This 'closing process' has been described in previous studies. The 'closing process' concept refers to the process of establishing standards and developing technology and solutions for the ability to nationally control the reliability, integrity and availability of data transfer, storage and processing. The closing process is related to Internet fragmentation as a phenomenon (Kukkola, Ristolainen & Nikkarila 2017). For a more detailed presentation of Russia's information and cyber policies Cf. Ristolainen 2017.

[2] "A system of systems is a set of different systems so connected or related as to produce results unachievable by the individual systems alone. [...] They are capable of independent action. These constituents fulfil purposes of their own and can operate when disassembled from the whole. They are managed for their own purposes." (Krygiel 1999, p. 33-34). Bill Owens differentiates military information system-of-systems to components which enable "seeing", "telling", and "acting". (Owens 2001, p. 99).

view of military strategy (Kukkola, Ristolainen & Nikkarila 2017). It is preparing the battlefield for a state-to-state cyber conflict. Russia might aim to gain a decisive advantage in this cyber conflict by centrally controlling, protecting and monitoring its national segment of Internet and, if need be, by disconnecting it from the wider Internet.

The Russian system-of-systems of cyber security consists of multiple independent subsystems which have different functions and are controlled by various actors. The aim of this paper is to describe this system and to analyse its effects on the resilience of the national segment of Internet during different phases of conflict and thereby to provide information about what kind of military advantage it could provide to Russia. The paper begins by discussing how Russian academics and military leadership see the phases of international confrontation (*protivoborstvo*)[3], how these phases relate to government authority and how resilience[4] (*ustoichivost'*) of information systems connects to the concepts of security (*bezopasnost'*), manageability (*upravliaemost'*) and operational reliability (*nadezhnost'*). The paper continues by describing Russian national cyber security subsystems and their functions to get a clearer picture of the larger system which they are a part of. Then the paper proceeds to analyse this system-of-systems in four different phases of confrontation – peace time, intensified competition, conflict, and war – to get a better understanding of how Russia might benefit from the system it is building in different conflictual situations to maintain the resilience of its national segment of Internet. The paper concludes by discussing the possible effects of the Russia project for military strategic stability in cyberspace. This paper uses mainly Russian sources and previous research conducted by the author and his colleagues.[5]

Confrontation and resilience

The Russian concept of confrontation (*protivoborstvo*) characterises the Russian view on international relations. Russian theoretical thinking on information warfare divides relations into four stages: 1) 'peaceful coexistence' (*mirnoe sosushchestvovanie*); 2) 'conflict of

[3] The term has been translated to English as 'confrontation' (Cf. United States Defence Intelligence Agency 2017, 38) but 'struggle' might a better word as Ristolainen (2017) has argued. 'Struggle' has the advantage of side-stepping the definite line between war and peace and it emphasises the continuous character of adversary relations between states. Another alternative term could be 'countermeasures' as Russia seeks to argue that it has been historically under attack and is reacting defensively. This paper uses the term 'confrontation' because the objective is to emphasise the differences between phases of adversary relations.

[4] The concept is understood in this paper as the ability to prepare for, withstand, adapt and quickly recover from adverse cyber effects. (Cf. Vlacheas et al. 2011; European Comission 2018; Björck et al. 2017).

[5] Kukkola, Ristolainen and Nikkarila have previously approach Russian networks by comparing advantages and disadvantages in offence and defence between open and closed networks and argued that by closing, or disconnecting, its networks Russia gains a definite military advantage (Kukkola, Ristolainen & Nikkarila 2017).

interests' (*stolknovenie interesov*) or continuous 'natural rivalry' (*estestvennoe sopernichestvo*); 3) 'armed confrontation' (*vooruzhennaia konfrontatsiia*); 4) 'war' (voina) (Manoilo 2003, p. 276-277; Panarin & Panarina 2003, p. 20-21). According to Evgenii Shalamberidze confrontation more generally is defined as "the actions of subjects of international relations to resolve their disagreements." It is divided into peaceful relations where non-violent means of confrontation are used; into foreign policy conflict where non-violent and violent direct and indirect non-military and indirect military means are used, and into military conflict where all means are used, primarily direct military (Shalamberidze 2011a, p. 28; Shalamberidze 2011b, p. 38-39). Chief of the General Staff of the Russian armed forces Valeri Gerasimov has presented a somewhat similar vision of the development of modern interstate conflicts or 'new type of war'. He emphasized the use of non-contact means against critical infrastructure objects in all dimensions of warfare (Gerasimov 2013). Later, General-Lieutenant Andrei Kartapalov argued that West was preparing to use this 'new type of war' against and Russia, as the weaker belligerent, should respond with 'asymmetric operations' i.e. using vulnerabilities of the enemy to negate its strength with minimal expenditure of resources (Kartapalov 2015, p. 35-36). Information means (including psychological and technological) are used in all phases of confrontation, but the use of open, kinetic or violent information means increase when confrontation moves towards war. Russia should include counteracting these threats to its deterrence (*sderzhivanie*) (Dylevskii et al. 2016).

On the official side, the Russian military doctrine differentiates national security situation between the peace time, the time of immediate aggression, and the war time (The Military doctrine of the Russian Federation 2014, p. 22). The Russian law also recognizes the concepts of 'the state of emergency' and 'the state of war' which are both connected to security threats against the state. The former gives the state the authority to restrict the freedom of mass communications, to increase the protection of objects vital to the population, and to manage the use of public communication networks. The latter gives the state the authority to control communication systems (Federal'nyi zakon 2002, p. VII, 14-15; Federal'nyi zakon 2001, p. XII, v; Federal'nyi zakon 2003, p. X). Additionally, Russian law on mobilization mandates the preparation of the nation to war – including mobilization of material and personnel reserves – before the state of war has been declared (Federal'nyi zakon 1996, p. V, 4). Based on the Russian the understanding of the continuum of confrontation and associated legal concepts this paper uses the peace time, intensified competition, conflict and war as analytical contexts to examine the resilience of the Russian segment of Internet.

Russians use the word '*ustoichivost''* ('stability' in English) when they write about resilience as understood in Western sources. It has been described as the ability of a system to function under stress and to return to its normal state after disruption (Makhutov, Reznikov & Petrov 2014, p. 9). In a military context cyber resilience (*kiberustoichivost'*) has been described as the ability of an information-communication network to support command and control while under computer attack. Resiliency is seen as composed of survivability, reliability and resistance to noise. (Kotsyniak et al. 2015, p- 7-8). A more 'civilian' version of cyber resilience would be the ability of a computer network to ensure and support an acceptable level of service in adverse conditions (Kotentko 2017, p. 161). The term '*ustoichivost'*" is used in the current Information security doctrine in connection to the performance and integrity of the national communication networks (The President of the Russian Federation, 2016, IV, 23, g). It can be argued that the Russian concept of '*ustoichivost'*" is quite similar to Western concepts.[6] Because Russians have adapted the concept of resilience from Western sources there does not seem to be significant differences on a conceptual level (Cf. Lukatskii 2017).

In the framework of 'Digital economy' resilience is connected to the concepts of security, manageability and operational reliability (The Government of the Russian Federation 2018b). Security is connected to a wider concept of information security which incorporates the protection of individuals, society, economy and the state from psychological and technological threats. On a more concrete level it is connected to the countering of hostile propaganda and protection from and monitoring and responding to threats against CII (The President of Russian Federation, 2016). Manageability and reliability are more technical concepts and are connected to the control of Internet traffic and the duplication of CII services (The Government of the Russian Federation, 2018b). It is crucial to note that resilience of networks on a strategic level from a Russian perspective cannot only be approached as a technical issue (i.e. cyber issue). It is inherently connected to the will of the Russian people and to the ability of the government to function which are the supposed main targets of any kind of information operation (The President of Russian Federation, 2014 & 2016). This aspect forms the psychological side of resilience. The following analysis is based on the understanding that the system-of-systems described below is a means to achieve resilience, security, manageability and reliability of the national segment of Internet, which roughly corresponds to the Western concept of resilience, and is also a means to maintain the psychological side of resilience of a nation.

[6] Cyber resiliency has been defined by Ross et al. (2018) as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources."

The System-of-systems

Russian government control over its national segment of Internet differs from other authoritarian countries.[7] Internet in Russia has developed from bottom-to-top by somewhat unregulated private actors (Soldatov & Borogan 2015), but after 2012-2013 the Russian state has adopted a policy of top-to-bottom control for political, economic, and military reasons. Controlling measures related to those policies have divergent operators and functions and they work at various technological levels (Kukkola 2018b). This paper argues that these controlling measures can be analysed as subsystems of a system-of-systems meant for the controlling of the national Internet by the state. There is, in fact, a reason to believe that the Russians are striving for 'a unified information space', something that they did not manage during the Cold War, which basically means a horizontally integrated and centrally controlled national information network (Kukkola 2018c).

The first system of measures is composed of administrative and technical measures to remove from and restrict access to unwanted content in Internet, including banning of foreign Internet services. Additionally, there are efforts to remove anonymity from the Russian Internet by restricting the use of VPNs and by introducing digital identification. The function of this system is political control (Federal'nyi zakon 2003; Kukkola 2018a). *The second system* consists of a targeted surveillance system SORM-3 and massive Internet data traffic retention by ISPs. They enable traffic and content-based analysis of security threats and appropriate actions by security services. The function of this system is internal security and political control (Soldatov 2017). *The third system* is an economic mechanism based on export substitution. It aims to replace foreign hardware, software and encryption solutions in Russian public and private spheres. System's primary function is to create domestic digital economy but also to achieve security through obscurity and, inversely, internal security through transparency – security services might have access to backdoors and encryption keys of domestic products (The Government of the Russian Federation, 2017; Kukkola 2018a). *The fourth system* is a nation-wide state led information infrastructure project including global satellite network that could provide Internet to remote areas and in the case of disruption of traffic in fibreoptic backbone networks. Infrastructure will be owned by state-controlled companies and it is reasonably to argue that

[7] China's system is currently based on political censorship and societal control, and the state has controlled the development of Internet from the beginning. Countries like Iran and Egypt have controlling mechanism based on technical solutions but do not comprehensive strategy for controlling national segment of Internet (Drake, Cerf & Kleinwächter 2016).

the architecture build by these companies will serve the strategic interests of the state. The official function of this system is to bring Russian society to the information age, but it also allows state to shape how the physical information infrastructure is build and connected (The Government of the Russian Federation, 2018c; Roskomsvoboda 2018).

The fifth system is based on the state control of CII - including Internet infrastructure. This system, on the one hand, is based on a law which designates the responsibility of protecting CII to private sector but gives the state administrative control of CII and, on the other hand, includes direct state ownership of certain elements of infrastructure through state owned companies and national duplication critical Internet services. System's official function is to protect CII but it also gives indirect or direct control of CII to the state (Federal'nyi zakon 2017; The Government of the Russian Federation 2018). *The sixth system* consists of a network of national SIEM (Security Incident and Event Management) systems and a network of national CERTs. The system will be deployed in public and corporate networks. Its function is to enable national centrally and vertically controlled system of monitoring, incident management and response of the national segment of Internet (Kukkola 2018a & 2018b). *The seventh system* consists of state control of Internet traffic routing on physical and logical levels which aims to create a basis for separated, and if needed closed, Russian segment of internet. This is achieved through direct state ownership of CII and through laws regulating the private sector. System's function is to enable the closing of national segment of Internet (Kukkola & Ristolainen 2018).

If the Russian government manages to combine the above discussed subsystems to a system-of-systems, it gains centralized control of the national segment of Internet. This capability will, among other things, significantly enhance the segment's technical resilience, and allows the state to flexibly react to changes in information warfare in separate phases of international confrontation. It also increases its ability to defend against the psychological aspect of information warfare.[8]

The Battlefield

The use and benefits of the potential Russian system-of-systems of cyber security and defence measures vary depending on the level of confrontation and the threats arising from it. In a

[8] Russian academics have written about the benefits of unifying the different protection mechanisms of the national segment of Internet, so the claims made in this article are based on ideas discussed by the Russians themselves (Cf. Kotsyniak et al. 2015, 116; Pilyugin 2017).

normal time, when the means used are primarily non-violent and psychological the first and second subsystems provide adequate means of resilience. Additionally, at this point of relations up until the state of war the whole system-of-systems functions as a deterrence mechanism – communicating inflated costs to a potential attacker or at least decreased effectiveness. Subsystem three makes espionage and exploitation more difficult and as such increases the costs for would-be aggressor. At this point national network can be considered as 'monitored' which is the basis for resilience i.e. the preparation for withstanding and recovering from disturbance.

At the second phase of confrontation, there is a clear and present danger and operations against the national segment of the Internet have increased although the means used are still covert, indirect, and non-military. The situation might call for 'a state of emergency' or at least increased intervention of the state to the functioning of Internet. Subsystems one and two are fully activated and subsystem three works in the background. Subsystems five and six are now activated in a centrally controlled manner. They are used to monitor, counter and attribute aggressive operations. This increases the resilience of the national segment but additionally allows Russia to, in the best case, name-and-shame the attackers. The ability to monitor the rising threats against critical infrastructure and to counter exploitation operations (meant for future attacks) gives the state a definite advantage when individual private sector actors are not left alone to fed off attacks. It also provides a better situational awareness. This helps the state to prepare for the potential future cyberattacks. At this point the national network is 'controlled' and is prepared to withstand a wider and more aggressive attack and both technological and psychological effects are kept in check.

At the third phase of confrontation the threat has materialized, and the aggressor has been very likely identified. Aggressor has shifted from espionage and exploitation to direct attacks against CII and the psychological element in the attacks might have lessened. All the previously mentioned subsystems are functioning at full strength. If they fail to provide adequate protection or if the aggressor tries to undermine the basis of Russian information society by bringing down or disconnecting the whole national segment of Internet from the outside, subsystem seven is deployed to disconnect the segment in a controlled manner. This decreases significantly the possible attack vectors and outside psychological information operations are greatly restricted. Additionally, traffic inside the segment is heavily controlled and monitored which increases protection against insider attacks. State now has the full control of the national segment of Internet and the private sector is mobilized to sustain critical services needed for the functioning of the government, the military, and the basic services for the citizens. Adaptation and recovery are provided by the interaction of all subsystems. At this point the national network is ‘closed’.

At the fourth phase of conflict the state has been mobilized for total war. The aggressor is using all means available to disrupt, degrade and destroy Russian CII with both non-kinetic and kinetic direct means. Some of the subsystems probably lose their functionality because of the damage inflicted by the aggressor. Subsystem four enables the Russian state to withstand this phase of confrontation – as Internet, in fact, was originally supposed to do in the United States (Kaplan 2016). Satellites, fibreoptic cables, radio frequency-based technologies, and dispersed server farms enable the national segment of Internet to fragment but still function in coherent, territorially based manner. Military is provided with connectivity in separate theatres or directions of war and nuclear weapons can be launched in a controlled manner. Separated parts of the national segment are still resilient to a certain extent thanks to modular nature of subsystems. At this point the national network is ‘fragmented’ but still resilient in its parts.

From the above analysis it seems believable that Russia might benefit from the system-of-systems of cyber security and defence measures. It would be able to maintain technological resilience of its networks and to counter psychological operations. Russia would gain this advantage, in theory, with minimal costs by imposing controlling mechanisms upon a network already built by private sector or by state-controlled companies in the context of ‘Digital economy.’ Perhaps the most interesting thing is that the system would be useful in deterrence and in countering both the so-called ‘colour revolutions’ and open military aggression in the form of ‘non-contact war’ (Gerasimov 2013; Kartapalov 2015).

Conclusions

Internet is fragmenting as authoritarian states are imposing their view of sovereignty on cyberspace. Although there are many aspects in this process, the military strategic one should not be bypassed. By creating a system-of-systems of cyber security and defence measures Russia strives to create a unified national network which could provide it a definite, even asymmetric, advantage in multiple ways. Resilience is one way to analyse this advantage. Flexible, centrally controlled system could enable Russia to counter various information threats in different phases of conflict. Nevertheless, it should be kept in mind that cyberspace, and the Internet as a part of it, is inherently connected and the services it provides do not easily conform to sovereign territories of states. The kind of system-of-systems Russia might be striving for is quite complex both in technological and bureaucratic sense. It could also hamstring the development of digital economy in many, perhaps unseen, ways. There is additionally the inherent risk to be considered of any centrally controlled system to be vulnerable by its very nature. For example, an antagonist might be able to disable the central controlling apparatus by using zero-day vulnerability in the control protocols of the system-of-systems and paralyze it.

Resilience has become somewhat of a catchword in cyber issues after it has been accepted that the attacker has the advantage. The only way to negate this advantage is to withstand the attack and recover as quickly as possible. If Russia manages to build up a system that allows it to do this on a national level, it will have a defined advantage. What is more important is that while its networks keep working and psychological effects are negated, aggressors might not have a similar advantage. This changes the balance of power in cyberspace. But what is perhaps more important is that the Russian system in explicitly based on an authoritarian view of cyberspace and Internet. By copying it other states implicitly concede to Russian view of political relations in and between states. If the Internet is fragmenting, those states that want to uphold democratic freedoms have to come up with a solution to this military-strategic challenge which does not lead them to give up on their basic values.

References

Björck, Fredrik, Henkel, Martin, Stirna, Janis & Jelena Zdravkovic, 2015. Cyber Resilience – fundamentals for a definition. In Advances in Intelligent Systems and Computing, vol. 353, 311-316.

Demchak, Chris & Dombrowski, Peter, 2014. “Cyber Westphalia: Asserting state prerogatives in cyberspace”, The Georgetown Journal of International Affairs, No. 20, pp 29-38.

DeNardis, Laura, 2014. The Global War for Internet Governance. London: Yale University Press.

Dylevskii, I. N., Zapivakhin, V. O., Komov, S. A., V. S. Korotkov & A. A. Krivchenko, 2016. O dialektike sderzhivaniia I predotvrashcheniia voennykh konfliktov v informatsionnuiu eru. Voennaia Mysl’ No. 7 July 2016, 3-11.

Drake, William J., Cerf, Vinton G. & Kleinwächter, Wolfgang, 2016 Internet Fragmentation: An Overview. World Economic Forum [Online]. Available from: https://www.weforum.org/reports/internet-fragmentation-an-overview [Accessed 6 June 2018].

European Comission 2018. Building Resilience: The EU's approach – Factsheet. [Online]. Available from: http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/resilience_en.pdf [Accessed 10 June 2018].

Federal’nyi zakon, 1996. “Ob oborone” No. 61-F3 (red. ot 29.12.2017). [Online]. Available from: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=286966&rnd=5412D87B6D386DDD8A34888AFCA04744#08631635764800438 [Accessed 10 June 2018].

Federal’nyi zakon, 2001. “O chezvychainom polozhenii” No. 3-FK3 (red. ot 03.07.2016). [Online]. Available from: http://www.consultant.ru/document/cons_doc_LAW_31866/ [Accessed 10 June 2018].

Federal’nyi zakon, 2003. “O sviazi” No. 126-FZ (red. ot. 05.12.2017). [Online]. Available from: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=284294&fld=134&dst=417,0&rnd=0.1557327116187115#0 [Accessed 11 January 2018].

Federal’nyi zakon, 2002. “O voennom polozhenii” No. 1-FK3 (red. ot. 01.07.2017). [Online]. Available from: http://www.consultant.ru/document/cons_doc_LAW_35227/ [Accessed 10 June 2018].

Federal'nyi zakon, 2017. “O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiyskoi Federatsii”, No. 187-FZ, [Online]. Available from: http://www.consultant.ru/document/cons_doc_LAW_220885/ [Accessed 1 November 2017].

Freedom House, 2017. Freedom on the Net 2017: Russia. [Online]. Available from: https://freedomhouse.org/report/freedom-net/2017/russia [Accessed 11 January 2018].

Gerasimov, Valerii, 2013. Osnovnye tendentsii razvitiia form i sposobov primeneniia vooruzhennykh cil, aktual’nye zadachi voennoi nauki po ikh sovershenstvovaniiu. Vestnik Akademii voennykh nauk, 42(1), pp. 24-29.

Kallberg, Jan, 2016. Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations. The Cyber Defense Review, 1(1) (Spring 2016), pp. 113-128.

Kaplan, Fred: Dark Territory. The Secret History of Cyber War, Simon & Schuster, New York, 2016.

Kartapalov, Andrei, 2015. Uroki voennykh konfliktov, perspektiby razvitiia sredstv i sposobov ikh vedeniia. Priamye i nepriamye deistviia v sovremennykh mezdunarodykh konfliktakh. Akademii voennykh nauk, 51(2), pp. 26-36.

Kotsyniak, M. A., Kuleshov, I. A., Kydriavtsev, A. M. & O. S. Lauta, 2015. Kiberustoichivost’ informatsionno-telekommunikatsionnoi seti. Saint Petersburg: Boston-spektr.

Kotenko, V. I., Saenko, I. B., Kotsyniak, M. A. & O. S. Lauta, 2017. Otsenka kiberustoichivosti komp’iuternykh setei na osnove modelirovaniia iberatak metodom preo’razovaniia stokhasticheskikh setei. SPIIRAS Proceedings 2017, 6(55), pp. 160-184.

Krygiel, Annette J., 1999. Behind the Wizard’s Curtain: An Integration Environment for a System of Systems. CCRP Publication Series.

Kukkola, Juha, 2018a. New guidance for preparing Russian ‘digital sovereignty’ released. Finnish Defence Research Agency Research Bulletin 01 – 2018 [Online]. Available from: http://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+Tutkimuskatsaus+1-2018.pdf [Accessed 6 June 2018].

Kukkola, Juha, 2018b. Civilian and military information infrastructure and the control of the Russian segment of Internet. Paper presented to ICMCIS 2018, Warsaw 22.-23. May 2018.

Kukkola, Juha, 2018c. Russian Cyber Power and Structural Asymmetry. In Chen, Jim Q. & Hurley, John S. Proceedings of the 13th International Conference on Cyber Warfare and Security. National Defense University Washington DC, 8.-9. March, 362-368.

Kukkola, Juha, Ristolainen, Mari & Nikkarila, Juha-Pekka, 2017. Game Changer. Structural transformation of cyberspace. Riihimäki: Finnish Defence Research Agency [Online]. Available from: http://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+julkaisuja+10.pdf/5d341704-816e-47be-b36d-cb1a0ccae398 [Accessed: 9 April 2018].

Kukkola, Juha & Ristolainen, Mari, 2018. Projected territoriality: A case study of the infrastructure of Russian ’digital borders’. Paper to be presented to ECCWS 2018, Oslo, 28.-29. June 2018 [Forthcoming].

Lukatskii, Aleksei, 2017. Kiberustoichivost’, kiberzhivuchest’, kiberhadezhnost’, kibernepreryvnost’. SecurityLab Blog [Online]. Available from: https://www.securitylab.ru/blog/personal/Business_without_danger/342751.php [Accessed 13 June 2018].

Libicki, Martin C., 2016. Cyberspace in Peace and War. Annapolis: Naval Institute Press.

Lin, Herbert 2011. Operational Considerations in Cyber Attack and Cyber Exploitation. In Deveron, Derek. S. Cyberspace and National Security. Washington, DC: Georgetown University Press, pp. 37-56.

Makhutov, N. A., Reznikov, D. O. & Petrov, V. P., 2014. Osobennosti obespecheniia bezopasnosti kriticheskikh infrastruktur. Besopasnost’ v tekhnosfere, No. 1 (January-February 2014), pp. 3-14.

Manoilo, A.V., 2003. Gosudarstvennaia informatsionnaia politika v osobykh usloviiakh. Moscow: MIFI.

Mueller, Milton, 2017. Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace, Cambridge, UK: Polity.

Musiani, Francesca, Cogburn, Derrick L., DeNardis, Laura & Nanette S. Levinson (eds.), 2016. The Turn to Infrastructure in Internet Governance. New York: Palgrave Macmillan.

Ross, Ron, Graubart, Richard, Bodeau, Deborah & Rosalie Mcquaid, 2018. Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure

Systems. Draft NIST Special Publication 800-160 Volume 2 [Online]. Available from: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf [Accessed 13 June 2018].

Nye, Joseph S. Jr., 2011. The Future of Power. New York: PublicAffairs.

Panarin I. & Panarina L., 2003: Informatsionnaia voina i mir. Informatsionnoe protivoborstvo v sovremennom mire. Moscow: OLMA-PRESS.

Pilyugin, P., 2017. ”Problemy opredeleniia granits v informatsionnom prostranstve”, T-Comm: telekommunikatsiia i transport, 11(8), pp 37-44.

Rid, Thomas, 2013. Cyber War Will Not Take Place. London: Hurst & Company, 2013.

Ristolainen, Mari, 2017. “Should ‘RuNet 2020’ Be Taken Seriously? Contradictory Views about Cyber Security Between Russia and the West,” Journal of Information Warfare, 16(4), pp. 113-131.

Roskomsvoboda, 2017. "Kitaizatsiia" Runeta vkhodit v aktivnuiu fazu i nachetsia s tochek obmena trafikom. 18 August 2017 [Online]. https://roskomsvoboda.org/31224/ [Accessed 21 January 2018].

Roskomsvoboda, 2018. Rostelekom gotov ychastvovat’ v razrabotke rossiiskogo kocmicheskogo interneta. 24 May 2018 [Online]. Available from: https://roskomsvoboda.org/39171/ [Accessed: 12 June 2018].

Shalamberidze, E. G., 2011a. Nepriamoe protivoborctvo v sfere voennoi bezopasnosti v usloviiakh mirnovo vremeni. Vestnik Akademii voennykh nauk, 34(1), pp. 20-30.

Shalamberidze, E. G., 2011b. Teoreticheskie voprosy razvitiia politiki natsional'noi oborony Rossii v usloviiakh mirnogo vremeni s ispol'zovaniem sistemy mer nevoennogo i voennogo kharaktera. Vestnik Akademii voennykh nauk, 37(4), pp. 35-43.

Soldatov, Andrei, 2017. The Taming of the Internet. Russian Social Science Review, 58(1) January–February 2017, 39-59.

Soldatov, Andrei & Borogan, Irina, 2015: The Red Web. The Struggle Between Russia's Digital Dictators and The New Online Revolutionaries. New York: Public Affairs.

The Government of the Russian Federation, 2017. Programma “Tsifrovaia ekonomika Rossiiskoi Federatsii” No. P-1632-p 28 July 2017 [Online]. Available from: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf [Accessed 22 September 2017].

The Government of the Russian Federation, 2018a. “Ob utverzhdenii Pravil kategorirovaniia ob’’ektov kriticheckoi informatsionnoi infrastuktury Rossiiskoi Federatsii” No. 127 8 February 2018 [Online]. Available from: http://www.consultant.ru/document/cons_doc_LAW_290595/ [Accessed: 6 June 2018].

The Government of the Russian Federation, 2018b. “Plan meropriiatii po napravleniiu ”Informatsionnia bezopasnost’” programmy ”Tsifrovaia ekonomika Rossi-iskoi Federatsii”.” Appendix N. 4 to the minutes of the meeting 18 December 2017 [Online]. Available: http://static.government.ru/media/files/AEO92iUpNPX7Aaonq34q6BxpAHCY2umQ.pdf [Accessed: 22 March 2018].

The Government of the Russian Federation, 2018c. “Plan meropriiatii po napravleniiu “Informatsionnaia infrastruktura” programmy “Tsifrovaia ekonomika Rossiiskoi Federatsii”.” Appendix N. 3 to the minutes of the meeting 18 December 2017 [Online]. Available from: http://www.consultant.ru/document/cons_doc_LAW_287865/ [Accessed: 22 March 2018].

The President of the Russian Federation, 2014. Voennaia doktrina Rossiiskoi Federatsii, No. Pr-2976 25 December 2014. [Online]. Available from: http://kremlin.ru/supplement/461 [Accessed 10 June 2018].

The President of the Russian Federation, 2016. Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii, N 646 5 December 2016 [Online]. Available from: http://rulaws.ru/president/Ukaz-Prezidenta-RF-ot-05.12.2016-N-646/ [Accessed 12 June 2018].

The United States Defense Intelligence Agency, 2017. United States Defense Intelligence Agency report: Building a military to support great power aspirations, Defense Intelligence Agency, viewed 2 August 2017, http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf [Accessed 13 June 2018].

Valeriano, Brandon & Maness, Ryan C., 2015. Cyber War versus Cyber Realities: Cyber Conflict in the International System. Oxford: Oxford University Press.

Vlacheas, Panagiotis T., Stavroulaki, Vera, Demestichas, Panagiotis, Cadzow, Scott & Slawomir Gorniak, 2011. Ontology and taxonomies of resilience. ENISA. [Online] Available from: https://www.enisa.europa.eu/publications/ontology_taxonomies/at_download/fullReport [Accessed 10 June 2018].