22nd International Command and Control Research and Technology Symposium
6-8 November – Los Angeles, USA

Topic 9: Battlefields of the Future

Asymmetric frontlines of cyber battlefields

Captain, M.Soc.Sci, Juha Kukkola
National Defence University
P.O. Box 7, FI-00861 Helsinki, Finland
juha.kukkola@mil.fi

First Lieutenant (Eng.), PhD, Juha-Pekka Nikkarila
Finnish Defence Research Agency
P.O. Box 10, FI-11311 Riihimäki, Finland
juha-pekka.nikkarila@mil.fi

Researcher, PhD, Mari Ristolainen
Finnish Defence Research Agency
P.O. Box 10, FI-11311 Riihimäki, Finland
mari.ristolainen@mil.fi

ASYMMETRIC FRONTLINES OF CYBER BATTLEFIELDS

ABSTRACT: The fragmentation of the global network progresses towards a formation of national segments of cyberspace walled with 'digital borders'. A number of nations aim to strengthen their sovereignty over the internet by closing their national networks. Russia and China are so far the most powerful nations to implement the closing process. The existing formats for internet governance are becoming outdated, which is followed by an unavoidable threat towards the remaining open-network society – there is no clear line between the concepts of war and peace in cyberspace. In this paper we intend to show how 'digital sovereignty' could be technically structured, what kind of policies it requires and how it would affect future cyber battlefields. 'Digital sovereignty' combined with the ambiguity of conflict creates an asymmetry that can be exploited and used for shaping the cyber domain into a future battlefield with 'asymmetric frontlines'. We claim that the conventional understanding of asymmetry in cyberspace that is based on the problem of attribution will be outdated. Furthermore, our analysis demonstrates how space and time variables form a base for asymmetry in the cyber battlefield of the future. By studying, on the one hand, the creation of asymmetry and on the other its effects on the freedom of action, decision-making and situation awareness of the belligerents, we analyze the creation and dynamics of 'cyber asymmetry'. The overall aim of this paper is to consider what a future cyber battlefield will look like and, at the same time, to improve cyber situation awareness related to the closing process. Finally, we suggest new strategic dilemmas for future study.

Keywords: Battlefield of the Future, Cyber Domain, Digital Sovereignty, Open-Network Society, Closed-Network Nation, Asymmetric Frontlines, RuNet

1. INTRODUCTION

The fragmentation of the global network progresses towards the formation of national segments of cyberspace[1] walled with 'digital borders'[2]. A number of nations aim to strengthen their sovereignty over the Internet by closing their national networks, i.e. the race for 'digital sovereignty'[3] has begun. Russia and China are so far the most powerful nations following the closing process[4] (Freedom House 2016; Inkster 2016). The existing formats for Internet governance are becoming outdated, which is followed by an unavoidable threat towards the remaining open-network society[5]. Cyberspace is artificial and can be shaped. Thus, it functions as a platform for a new type of asymmetry. Moreover, the current paradigms of conflict have been challenged – there is no clear line between the concepts of war and peace in cyberspace (cf. Russian 'information counter struggle'[6]). These processes together create tension that increases the probability for nation-state

[1] In this paper the concept of 'cyberspace' is defined as "an electronic medium through which information is created, transmitted, received, stored, processed and deleted" (Critical terminology foundations 2 2014, 17). We use separate concepts for 'cyberspace' and 'cyber domain' (cf. footnote 9).

[2] The concept of a border is confusing in the 'borderless' cyberspace. There is no common understanding what borders in cyberspace are or what concept to use (e.g. 'cyber border', 'virtual border', 'unspatialized border', 'iBorder' etc.). In this paper we have decided to use the concept 'digital border', firstly, because it is a direct translation of a concept used in Russian (*tsifrovaia granitsa*) and secondly, the word 'digital' reflects 'computer technology' and 'data processing'. In our understanding, a 'digital border' represents an entity that separates potential national segments of the cyberspace.

[3] In the Russian approach, 'digital sovereignty' is envisioned as the right and ability of the national government to independently determine national interests in the digital environment (Ashmanov 2013), i.e. cyberspace.

[4] The concept of a 'closing process' refers to the process of establishing standards and developing technology and solutions for the ability to nationally control the confidentiality , integrity and availability of data transfer, storage and processing. The closing process is related to Internet fragmentation as a phenomenon.

[5] An open network (i.e. global Internet) is defined in this paper as a network based on a multi-stakeholder process, non-nation based governance, public-private partnerships, open access and global connectivity. The open network represents part of the global commons – a collective asset that secures freedom of expression, media pluralism, and equal access to knowledge etc. (Chouri 2012, 221-238). An open-network nation shares the values of open networks and its segment of the Internet is built on those principles. An open network-society is a collection of the above defined nations. The concepts of an open network, an open-network nation and an open-network society are used without quotation marks hereafter.

[6] Russia has activated a concept called 'information counter struggle' (*informatsionnoe protivoborstvo*) (Doktrina 2016) that has been inaccurately translated and interpreted as 'information war' in numerous Western studies on Russian cyber strategies. The fundamental problem is that 'information counter struggle' has never been solely limited to wartime (Ristolainen 2017). Initially, Russian theoretical thinking divides 'information counter struggle' into four stages: 1) 'peaceful coexistence' (*mirnoe sosushchestvovanie*); 2) 'conflict of interests' (*stolknovenie interesov*) or continuous 'natural rivalry' (*estestvennoe sopernichestvo*); 3) 'armed confrontation' (*vooruzhennaia konfrontatsiia*); 4) 'war' (*voina*) (Manoilo 2003, 276-277; Panarin & Panarina 2003, 20-21).

confrontation in cyberspace. The overall aim of this paper is to consider what a future cyber battlefield will look like and, at the same time, to improve cyber situation awareness related to the closing process. Finally, we suggest new strategic dilemmas for future study.

We will continue and deepen the analysis of the potential impact of a closed national network[7] to cyberspace (Ristolainen 2017, Nikkarila & Ristolainen 2017, Kukkola et al. 2017).[8] In this paper we are interested in studying how 'digital sovereignty' could be technically structured; what kind of policies it requires; and, how it would affect future cyber battlefields. 'Digital sovereignty' combined with the ambiguity of conflict creates an asymmetry that can be exploited and used for shaping the cyber domain[9] into a future battlefield[10] with 'asymmetric frontlines'[11]. We analyze the formation of imminent 'cyber asymmetry'[12] by a closed-network nation. We claim that the conventional understanding of asymmetry (cf. Libicki 2009) in cyberspace, which is based on the problem of attribution[13], will be outdated in future battlefields. Our hypothesis is that by creating new frontlines on the cyber battlefields, belligerents can shape battlefield space and time to their advantage. The space and time variables form a base for asymmetry on the future cyber battlefield.

The scope of this paper is limited both temporally and technically. Our focus is on the 'gray zone' (Barno & Bensahel 2015, Votel et al. 2016), and the 'initial period of war'[14] of cyber conflict. That is, the politically ambivalent, militarily restricted and normatively under-regulated continuum that extends from nation state competition all the way to the first open use of armed force. We have restricted our study to using existing protocols: Border Gateway Protocol (BGP) (Request for Comments (RFC) 7426) combined with networking architecture Software Defined Networking (SDN) (RFC 4271) as probable (but not exclusive) technical solutions behind a closed national network (cf. Streltsov & Pilyugin 2016). Although we focus on Russia in this paper, we are open to the notion that our observations could also be applied to other states.

This paper is organized into conceptual and practical parts. In the conceptual part we, firstly, discuss the Russian ambition for 'digital sovereignty'. Secondly, the potential technical solutions for 'digital sovereignty' are explained. Thirdly, the concept of asymmetry is described from different viewpoints. In the practical part we, firstly, present an analytical approach to analyzing cyber asymmetry. Secondly, asymmetry is analyzed through battlefield space and time variables in different types of battlefield scenarios. Thirdly, we present a forecasting model for asymmetric frontlines in the cyber battlefield of the future. And as a conclusion, we will discuss how an open-network society can manage the asymmetry manipulated by a closed-network nation. The main contribution of this paper to the discussions is our analysis of the 'asymmetric frontlines' of future cyber battlefields. The overall aim of this paper is to improve situation awareness in the cyber domain and to suggest new strategic dilemmas for future study.

[7] The concept of a 'closed-network nation' is understood in this paper as a nation that is technically able to maintain a closed network, i.e. to operate a nationally governed segment of the Internet that can be technologically separated from the global Internet. The concept is used without quotation marks hereafter.

[8] In our previous studies, we have discussed the Russian approach to 'digital sovereignty' and the formation of the Russian national segment of the Internet by 2020, i.e. 'RuNet 2020' (Ristolainen 2017). Moreover, we have analysed the possible military aims of 'closed-network nations' and have come to the conclusion that their goal is related to enhancing military capabilities (e.g. the basic elements of combat power) when compared with open networks. In other words, it is likely that the motivation of a closed-network nation is to reach a higher operational capability than an 'open-network society' (Nikkarila & Ristolainen 2017). Furthermore, we have continued to analyse the outcomes of the closing process from the open-network society's point of view and shown how a closed-network nation can shape the cyber domain to gain an advantage and thus, may control the cyber domain and is able to force an open-network society into reactive mode. We have determined an open-network society's choices and their consequences in the case of escalation and potential confrontation (Kukkola et al. 2017).

[9] The concept of a 'cyber domain' is understood here as an operational domain that cuts across all strategic domains (land, sea, air and space) and has an effect on all other operational domains and is affected by them (NATO 2013; Libicki 2009). In our lexicon 'cyber domain' belongs to military terminology; whereas 'cyberspace' is a common platform (cf. footnote 1).

[10] In this paper the concept 'battlefield' is understood as a space where military operations are conducted. A 'cyber battlefield' is understood as the digital dimension of a conflict between opposing forces in the cyber domain where military operations are conducted.

[11] Simply, the concept of a 'frontline' is the occupied line that is closest to the enemy. In this paper an 'Asymmetric frontline' is defined as a line of contact that is situated differently for belligerents and gives one of them a clear advantage.

[12] In this paper 'cyber asymmetry' is based on shaping of cyberspace. 'Cyber asymmetry' affects the freedom of action, decision making and situation awareness of belligerents. The space and time variables play an integral part in 'cyber asymmetry'.

[13] The 'problem of attribution' is understood in this paper as a difficulty to identify a cause or a source of a cyber-attack that can be easily disguised.

[14] The term 'initial period of war' (*nachal'nyi period voiny*) and its variations are commonly used in Russian military texts. It emphasizes the need for preparation and decisive action in the first moments of armed conflict (Thomas 2016).

2. METHODS AND MATERIALS

Methodologically the conceptual part of this paper is a literature survey of writings pertaining to the Russian view of 'digital sovereignty'. Also, we use contextual analysis in order to explain the ambiguous 'asymmetry' concept used in 'Western' and Russian thinking, and military strategies. We do this by separating and explaining several aspects of asymmetry and then recombining them into a fresh and comprehensive understanding of 'cyber asymmetry'. As a result of the conceptual part, we will generate an analytical approach to comparative analysis of asymmetry in cyber domain.

In the practical part, we will use scenario analysis (cf. Kosow & Gaßner 2008) as an experimental methodology for understanding the context of 'cyber asymmetry' in different types of battlefields. Finally, we use forecasting modelling (cf. Coates & Glenn 2005; Martino 1993) of a cyber battlefield to define different asymmetric frontlines. Scenario analysis and forecast modelling are methodological approaches that allow us to work on the edges of our disciplinary boundaries and consequently, to combine Strategic studies, Russian studies, and IT technology studies into a study of cyberspace.

Our research material consists of previous Russian, military and cyber studies. One component of our main research material is an article called "About digital sovereignty" (in Russian) by Anatoly Streltsov and Pavel Pilyugin (2016). This work has given us both a conceptual and a technical framework. Additionally, will we use the following materials: the Russian National Security Strategy (2015); 2017-2020 Strategy for the Development of an Information Society in the Russian Federation (2017); and, Russian Information Security Doctrine (2016) that in our opinion reflect the potential events that could shape the future cyber battlefields.

3. 'DIGITAL SOVEREIGNTY' AND POST-WESTERN WORLD ORDER

'Digital sovereignty' as a concept has been part of the Russian 'information space'[15] discussion and research starting from 2012 (Dubov 2014, 125; Nocetti 2015, 113). One of the main visionaries behind the concept is an Internet technologies (IT) expert, Igor Ashmanov (2013), who has been envisioning 'digital sovereignty' as a right and an ability of the national government to independently determine geopolitical national interests in the digital environment. In 2016 it was declared that RuNet – the Russian segment of the Internet – would be disconnected from the global Internet by 2020 ('RuNet 2020') and in the Information Security Doctrine, Russia openly aims "to deploy a national system of managing the Russian segment of the Internet" (Doktrina 2016). Nevertheless, there are only a few Russian open source scientific studies on how to establish a closed-network nation and how it connects to achieving 'digital sovereignty' in practice. In their article Anatoly Streltsov[16] and Pavel Pilyugin[17] (2016) explain their view on the main components of 'digital sovereignty'; they give the technical parameters of how to maintain a nationally governed network; and, explain how their solutions would erase anonymity, i.e. the problem of attribution in a conflict situation. In the following we summarize Strelsov & Piyugin's (2016) designs and present the Russian legal and strategic thinking behind 'digital sovereignty' and explain the political motivation behind the network closing process.

3.1. Border control and governance of 'digital sovereignty'

Streltsov & Pilyugin (2016, 25-30) compare 'digital sovereignty' with traditional state sovereignty; they see the Internet as a federation of networks; and, apply simple border theory based on topography in cyberspace. Furthermore, they explain how there are certain rules of how national borders are to be protected and how different subjects (vehicles, goods, people, animals, etc.) can cross national borders. Streltsov and Pilyugin (2016, 28-29) suggest that 'digital sovereignty' requires the delineating of cyberspace, i.e. the formation of 'digital state borders'. Similarly, border crossing should be organized through 'digital border crossing points'

[15] In Russian 'cyberspace' is called 'information space' (*informatsionnaia sfera*) or 'information environment' (*informatsionnaia prostranstvo*), reflecting its extensiveness. The Russian information space includes all mass media, not only information and computer technology platforms. (Doktrina 2016.)

[16] Anatoly Streltsov – Deputy Director of the Institute for information security issues of the Moscow State University, doctor of technical sciences, doctor of legal sciences, professor.

[17] Pavel Pilyugin – senior researcher of the Institute of information security issues the Moscow State University, associate professor at Moscow Institute of Electronic technology, candidate of technical sciences.

where the incoming /outgoing (i.e. cross-border) traffic can be monitored. Moreover, they introduce the concept of 'digital customs'. 'Digital customs' would not check all the 'information packets' passing through the 'digital border', but the customs would have a right to monitor the "legitimacy of the information flow" (ibid, 28). For information security reasons, all of the programs used should be certified by national certification organizations. The national operators (i.e. providers) would be able to organize the traffic, but they would be under the control and supervision of the state. According to Streltsov & Pilyugin (2016, 29), all of this could be organized with existing technology by using BGP, a standardized exterior gateway protocol designed for exchanging routing and reachability information among autonomous systems (AS) on the Internet. Together with innovative use of e.g. SDN technology, states would be able to form their own policies and reach international or bilateral agreements for the 'digital border' crossing.

Streltsov & Pilyugin (2016, 29) complain that the contemporary control of Internet traffic based on national providers is technically simpler but it resembles more 'defense lines' than 'digital borders'. Without international agreements the future state cyberspaces will be connected with each other only through nationally controlled gateways, i.e. the Internet as a 'federation of networks' may turn into 'a confederation' (cf. Nikkarila & Ristolainen 2017). Moreover, Streltsov & Pilyugin (2016, 30) conclude their work by resolving the problem of attribution in cyberspace. They suggest that anonymity on the Internet can be erased by different nationally-controlled registration mechanisms of IP-addresses and domains and by state-owned providers of cross-border traffic authentication implementation.

3.2. Legal and strategic governance of 'digital sovereignty'

When reading Streltsov and Pilyugin's (2016) article in parallel with the recent Russian legal documents and changes in legislation we find indications that the measures suggested by Streltsov & Pilyugin (2016) could be the practical and technical solutions behind the Russian closed national network (cf. 'RuNet 2020'). For example, in 2016, the Russian Ministry of Communications and Mass Media (*Minkomsvyaz*) initiated a law drafting project preliminarily called 'About the Autonomous System of the Internet' (Golitsyna et al 2016). This project consists of two different proposals to update laws called 'On Communications' (Minkomsvyaz 2016) and 'On Information, Information Technologies and on Information Security' (Zakonoproekt 2017) that are closely related to the technical isolation of RuNet. In October 2016, Minkomsvyaz released a draft bill that defines basic Internet infrastructure concepts such as 'autonomous system' and 'infrastructure of the Russian national segment of the Internet' and 'national .ru and .рф zone domain name registrar' from the Russian point of view (Minkomsvyaz 2016). The draft bill mandates that the state would control RuNet's entire 'critical infrastructure', including the national .ru and .рф domains, Internet traffic exchange points (IXPs), as well as autonomous systems and networks. Furthermore, updates on the law 'On Information, Information Technologies and on Information Security' were implemented by the Federal Security Service of the Russian Federation (FSB) in December 2016 (Zakonoproekt 2017). The new bill titled 'On the Security of Critical Information Infrastructure of the Russian Federation' was approved at first reading in the state Duma in January 2017 and it will come into force in the beginning of 2018. It mandates that a special register of all companies and agencies that control objects of 'critical information infrastructure' must be formed. Taking all of the legislation for surveillance, control and isolation into account, it seems that a new official state register of IP addresses for RuNet might appear shortly and all of RuNet's 'critical infrastructure' and 'critical information infrastructure' will fall under the complete control of Russian state authors (Ristolainen 2017).

Overall, information security is part of Russian national security and an object of constant counter-struggle according to the Russian National Security Strategy (Strategiia 2015). Information security includes critical information infrastructure, technological self-sufficiency, political stability and 'spiritual values'. The role of government in securing the 'information sphere' is central (ibid). The Doctrine of Information Security (Doktrina 2016) states quite clearly that national security is linked to the 'information sphere', i.e. the sum total of technology, information and governance. Threats emanating this 'sphere' can affect even defense, sovereignty and the territorial unity of the Russian state. The military, and especially the intelligence services, have a role in the defense of these, but all in all information security is a centralized, government controlled, whole-of-government, top-down approach. The doctrine clearly sees the 'information sphere' as a space defined by information sovereignty, technological independence and territorial immunity (ibid).

The Doctrine of Information Security is partially implemented in the Strategy on the Development of Information Society in the Russian Federation for 2017-2030 (Strategiia 2017). The Strategy defines the 'information space' as the technological base of the 'information sphere' and also 'critical information infrastructure' as a collection of information systems, networks, and industrial control systems mainly used by the government and strategic enterprises.[18] The Strategy follows the Doctrine and takes a top-to-bottom approach to building an information society in Russia. The strategy states clearly that 'the Russian segment of the Internet' has to be nationally controlled, independent, self-sufficient, protected from outside interference, and under sovereign jurisdictions (ibid). Furthermore, the Strategy is executed, for instance, in a State Program 'Digital Economy of the Russian Federation', signed in July 28, 2017. It presents a 'road-map' tasking that Russia will be digitally sovereign by 2020 and that Russia will be one of the world's leading countries in the field of information security by 2024 (Tsifrovaia ekonomika 2017).

The idea emanating from these strategies and documents is clear. State sovereignty reaches into cyberspace and has its basis in the modern, territorial state. It is ideologically opposite to ideas about the global commons and the multi-stakeholder model of an open, safe, and secure Internet (Ristolainen 2017). These findings seem to be consistent with what Demchak and Dombrowski have called a 'Cyber Westphalia' i.e. territorialization of cyberspace (Demchak & Dombrovksi 2013).

3.3. 'Digital sovereignty' as a basis for post-western world order

It seems that Russia would prefer to treat 'cyber' as a geopolitical (or 'geodigital') territory. Thus, 'digital sovereignty' appears to be a logical concept for defining and safeguarding the borders of the Russian 'information space' and for ensuring 'information security'. According to Ashmanov (2013), the United States is the only country in the world that has a factual 'digital sovereignty'. In the Russian approach, the Internet is a by-product of the dominant American culture and therefore, proposes a threat to Russian cultural integrity and independence. The global Internet is dependent on popular applications and services that are provided by the United States based companies that pose a threat to Russian technological integrity and autonomy. Therefore, in the Russian mindset, an asymmetry has developed between Russia, the United States and the North Atlantic Treaty Organization (NATO) that influences the political, ideological, economic and technological fields (Kucheriavyi 2014). Consequently, there exists a long term and serious determination to challenge the US-dominated/led world order (Trenin 2016, 19) and progress towards 'a post-Western world order' (Lavrov 2017).

To summarize, from the Russian point of view the information space clearly belongs to the framework of state sovereignty. This means that there is a tendency to conceptualize it as a state-centric and territorial phenomenon, which is apparent in the effort to build the concept of 'digital sovereignty.' The external aspect of this Russian project is to challenge the world order that it perceives as Western and also, by using technical solutions to create a military advantage.

4. TECHNICAL SOLUTIONS FOR 'DIGITAL SOVEREIGNTY'

As noted in the previous chapter Streltsov & Pilyugin (2016) suggest that 'digital sovereignty' could be organized with existing technology by using BGP together with an innovative use of SDN technology[19]. In this chapter we will explain the technical details behind these and consider them as solutions for closing a national network. In the Russian academic field there has been a growing interest in these protocols over the past years, e.g. Krasotin & Alekseev (2013); Konstantinov et at. (2014)[20]; Chalyy et al. (2015)[21]; Sosenushkin &

[18] The strategy also gives Russian definitions to such modern concepts as IoT, Industrial Internet, Information society, eGovernment, Cloud computing, Big Data, Knowledge society, Digital economy, Fifth generation networks etc.

[19] It needs to be noted that theoretically the closing process could be successful by using solely BGP protocol.

[20] Konstantinov et al. (2014)'s study considers the issues of using an SDN. The authors have applied several SDN designs in order to enhance a computer cluster performance. They simulated (emulated) a real network and conducted a comparison on different SDN designs. Apparently they emphasize that simulations can be used in order to find out which SDN solution is most suitable for a specified task.

Kruglova (2015)[22]; Chemeritskii (2015)[23]; and, Patrushev (2016)[24]. Still, it has to be noted that even if SDN technology brings many benefits to network administration, it has vulnerabilities that weaken its security (cf. Scott-Hayward et al. 2013). The study of these vulnerabilities is not included in this paper.

4.1. Border Gateway Protocol (BGP)

The BGP is a protocol providing connectivity between two or more ASs (networks). It is based on Autonomous System Numbers (ASN) that are assigned by the Internet Assigned Numbers Authority (IANA). Basically, the BGP connects individually administered networks to the whole Internet. ISPs can manage one or multiple ASs, and they agree among themselves how these are connected and who routes what traffic. According to its RFC 4271, BGP is to exchange network reachability information with other BGP systems. The correct function of a BGP is based on the mutual trust between the BGP systems. The exchange of reachability information is done manually with updates and withdrawn messages. There is also a possibility to filter these messages (Cisco 2016). This makes it possible to cut connection at both ends of the BGP links or to change routing information very quickly if necessary (Renesys 2013; SANS 2016). The BGP is an unsecure protocol and it has been targeted by malevolent actors in the past. Attempts to make it more secure with encryption and authentication have stalled because of policy challenges and cost-effectiveness (NIST 2017).

In the context of Russia's network closing process[25], the connection and disconnection with the rest of the world could be implemented with a BGP. Because there are multiple Local Internet Registries (LIR) (ca. 1400) and ASNs (ca. 5800) in Russia (RIPE NCC 2017), this requires considerable coordination and monitoring in addition to setting up, and administrative and legal procedures. It can be realistically claimed that not all of the information infrastructure of Russian ISPs (etc.) managing those ASNs is located geographically in Russia. Some parts of the networks might even be physically and logically separated from national core networks.

4.2 Domain Name System (DNS) and DNS Security Extensions (DNSSEC)

The BGP is only one element behind the correct operation of the Internet. The Domain name system is a hierarchically distributed registry that provides conversion of host names to IP addresses. In practice, every client must be told where to find its Domain Name Server (DNS) if host names are to be used instead of IP addresses on the Internet. The original description of the DNS function can be found in (RFC 882) and (RFC 883). The utilization of DNS is progressing by updates (RFC 1034, RFC 1035, RFC 8020).

The DNS security extensions (DNSSEC) add data origin authentication, as well as the data integrity, to the DNS (RFC 4033, RFC 6014, RFC 6840). The root keys of the DNSSEC system are in the possession of the Internet

---

[21] Chalyy et al. (2015) bring confidentiality into focus. In other words, how confidentiality may be achieved in an SDN architecture where several agents use the same infrastructure. They propose a specific approach where the controller does not violate the confidentiality and to some extent even integrity.

[22] In their paper, Sosenushkin & Kruglova (2015) present an imitation model of a highly utilized network segment under the control of a software defined networking (SDN) controller. A series of modeling experiments is used to prove the efficiency of SDN technology usage for highly loaded network segments.

[23] In his dissertation, Chemeritskii (2015) studies and develops methods and tools for evaluating the properties of SDN for known configurations of its components and verifying the compliance properties of these specified routing requirements policies.

[24] Patrushev (2016) studies the development of service routing, a method of a global route optimization, QoS parameters that need to be taken into account when calculating the route, end-to-end delay of packet delivery, existing technologies of traffic management service centralized adaptive routing software defined networking.

[25] RuNet is built on the physical backbone connections provided mainly by five companies (Rostelkom, MegaFon, MTS, Vimpelkom and TransTeleKom). Optical fiber connects main population centers but microwave and satellite connections are import as well as cellular networks (RuBroad.ru 2014). There are hundreds of ISPs running networks and services although many are local (Provy.ru, 2017). These are connected in the data link layer by Internet traffic exchange points (IXPs) –the two biggest are MSK-IX (38 nodes with over 500 customer AS) and DataIX (18 nodes with over 150 customer AS) (MSK-IX 2017; DATAIX 2017). IXP infrastructure is mostly situated in the western part of Russia or along the Siberian railway route (RuBroad.ru 2014). Routing between ASs is done by BGP4. There are ca. 11 root-level DNS in Russia (Root-servers.org, 2017). MSK-IX is responsible for higher level names server cloud for .ru and .рф domains. It has nodes in 7 federal *okrugs* (i.e. districts) and also abroad. There are governmental and military networks that are more or less separated from private networks (RSNet) (Russian Federation - Official Russia 2017; Izvestia.ru 2016). Basically, the majority of the infrastructure is in private hands. The private sector is regulated quite strictly by the Ministry of Telecommunications, Roskomnadzor and FSB (Federalnyi zakon 2017). Filtering and black listing are the responsibility of the ISPs, but the government has a SORM-3 system for monitoring and intercepting traffic (Ermoshina & Musiani 2017). Currently RuNet, and the service industry based on it, is growing quite fast and Internet penetration among population is 71.3% (Yandex.ru 2016; Internet Live Stats 2017).

Corporation for Assigned Names and Numbers (ICANN) and stored securely in diverse redundant locations (ICANN 2017).

When it comes to the closing process of the network, the role of the DNS is to conduct address resolution inside RuNet between Russian controlled Top-Level Domains (TLDs) and lower level domains even when the connection to other TLDs is severed. This implies centrally administered national-zone-authority policies to maintain server connections. In this scenario DNSSEC might provide security against third party name-servers masquerading as legitimate name-servers. It is likely that Russia will continue applying DNS with their IP address resolution and construct their whole system accordingly, including the national control of the root keys of the DNSSEC system.

4.3. Software Defined Networking (SDN)

In recent years, there has been a rapidly growing interest in a network technology called Software Defined Networking (SDN) within both the academic community and the industry. An RFC was published on the subject in 2015 (RFC 7426). SDN is considered as an emerging paradigm of networking by separating the control logic of a network from the underlying routers and switches; promoting (logical) centralization of network control; and, introducing the ability to program the network (Kreutz et al. 2015). So far, Openflow (McKeown et al. 2008) is the only main protocol supporting the utilization of SDN in practice. With Openflow one may set up a communications protocol between the forwarding layer and different SDN controllers. If Russia pursues a closed network, it is expected that Russia will utilize SDN (via Openflow or a proprietary protocol) in order to execute its routing and control domestically. These solutions would provide a centrally controlled and automated administration of RuNet. Its usage to control an entire country's Internet traffic is likely to require more investigation.

4.4. Possible Russian solution for network closing

As we have stated in chapter 3.2 there is political will to create a national, self-sufficient Internet in Russia. Given time, the outer connections of this network can be controlled with the BGP and the interior network traffic can be controlled by SDN. There is a host of political and financial issues to be solved before this happens, but in an authoritarian country with considerable state participation in the economy and manipulation of public threat perceptions it is only a matter of time. In our understanding the parallel usage of the BGP protocol and the innovative application of SDN architecture is considered to be the most cost effective, easiest, and fastest method to close a national network.

A more extreme measure of control could be national and governmental control of IP addresses and cryptography. By nationalizing the Regional Internet Registry (RIR) services (IP address distributors), establishing a system of fixed addresses, controlling routing information (perhaps by developing local transport and network layer protocols); and, by transparent cryptography, the Russian government could control their national information space. Problems with attribution would be significantly reduced because of a better control and transparency of the ingress traffic into a national network (cf. Chapter 8). All traffic would be transparent for the government and only administratively approved subjects might operate in the network. Because of the economic, legal, political, and technical implications this approach would be costly and in the end it might not work as intended. (cf. Streltsov & Pilyugin 2016, 27.) Also, besides or as a replacement for SDN and BGP Russia could employ national, proprietary protocols which would provide security through obscurity to a certain point. In this paper, our focus is on the BGP protocol and SDN technology. However, our aim is to continue and deepen the analysis of the technical solutions behind 'digital sovereignty' in our future studies.

5. CYBERSPACE AND ASYMMETRY

Political ideas and decisions, governance techniques, and technical solutions form the basis for 'digital sovereignty.' When this sovereignty is claimed unilaterally, it can be considered as an attempt to create asymmetric advantage in cyberspace. This might be considered as the practical aspect of the military nature

of ‘Cyber Westphalia’ (Demchak & Dombrovksi 2013). Westphalian sovereignty employed by one state or bloc, but not others, could lead to a considerable military advantage.

Simply, the absence of symmetry creates asymmetry. Yet, the concept of asymmetry is ambiguous and mostly used without a proper understanding of its implications. In this chapter, we focus on ‘Western’ and Russian asymmetric thinking and military strategies and apply them to cyberspace. Firstly, we will discuss the characteristics of cyberspace. Secondly, we will examine asymmetry as a military theoretical concept. Thirdly, we will combine cyberspace with asymmetry and explore the potential causes of asymmetry in cyberspace. And fourthly, we will reflect on the shaping of cyberspace based on the Russian thinking of asymmetry and ‘digital sovereignty’.

5.1. Characteristics of cyberspace

The Internet forms the basic structure of cyberspace. Still, there is no widely accepted definition of cyberspace. Some definitions divide it into constituent parts or different levels. Some focus more on information flows or processes from a holistic point of view. Yet, others concentrate more on the administrational, governmental and legal side of this new, artificial and continually changing space (Sheldon 2013, 282-298; Lango 2016). At the turn of the millennium, some envisioned cyberspace as a space transcending the so-called Westphalian state system (Barlow 1996). This was supposed to be a part of the globalization process that would bring about the disappearance of modern nation states. From this point of view, cyberspace can be viewed as a global commons, a region open to all who have the capability to use it (Mitchell 2006; Betz & Stevens 2011).

The global commons thinking is a good starting point for understanding cyberspace as a region characterized by a kind of architecture and model of governance that is naturally symmetrical and flattens the differences in power.[26] Cyberspace can be viewed as a network without a center, flat and free of physical geography. Access to it is cheap and easy, so non-state actors can challenge states and states can use non-state actors as proxies. Distance loses its conventional meaning and time is counted in microseconds, so the ability to make decisions and act quickly is more important than the ability to physically project power. (Nye 2010; Sloan 2012, 90-91; Sheldon 2013, 309-310). This means that the resources needed to operate in cyberspace are different than in the physical world. Information, skill, and organization are more important than weapons, transport capabilities or massive manpower (Slayton 2016, 108).

From a military perspective, because cyberspace is partly a non-physical, manmade, malleable environment, its relation to other domains is special. Cyberspace penetrates through every other domain. Power can be projected from it, through it, and into it (i.e. kinetic strikes against data centers). Cyberspace is also dependent on other dimensions. There are no communications without cables, satellite links, and data centers (Sheldon 2013, 288-289). There is an ongoing debate, whether cyberspace has a strategic meaning or if it is only an enabling environment, providing support for using force in other domains (cf. CyCon 2016; Rid 2012; Stone 2013). From the global commons point of view cyberspace offers a neutral platform from which to project power globally and instantaneously without the need to worry about borders or national sovereignty. This platform is open to nation states and terrorists alike. It does not enhance the absolute power of non-state actors or weak states, but disperses power and opens new avenues for its use (Nye 2010, 9).

There have been attempts to define illegal actions, armed attacks, and warfare in cyberspace, but this process is still ongoing and has many challenges, cf. Tallinn Manual 2.0 (2017) and United Nation Convention on Cooperation in Combating Information Crimes presented by Russia (Draft 2017). The Internet is based on a multi-stakeholder model which means that the civil society and non-state actors have an interest in keeping cyberspace out of the control of nation states and supra-governmental authorities (Muller 2016). There is also the problem of attribution, which means that because of the way protocols work and the Internet is

[26] It should be pointed out that Joseph Nye Jr. (2010, 15-16) criticizes the notion of cyberspace as a ‘global commons.’ He proposes the term ‘regime complex’ because there are multiple organizations that regulate cyberspace. The Internet cannot be considered as public goods and a part of the space is in sovereign control.

structured, it is difficult to attribute attacks on information systems on any specific party (Carr 2012; Rid & Buchanan 2015). Non-governance and non-transparency create an area for different kinds of actors to conduct criminal and subversive operations quite freely.

A major part of the physical infrastructure of cyberspace is owned by private companies, which follow commercial logic and try to stay out of international or local power struggles. Many of the basic services needed for the operation of the Internet are provided by Non-Governmental Organizations (NGOs). Software is produced by international companies (Muller 2016). What this means is that it is difficult for an actor or group of actors to try to 'conquer' or force their will on any part of cyberspace (Libicki 2009, 35). This digital landscape is constantly changing and resists attempts to control it. Information flows through the path of least resistance. In this context coercive power is based on influencing systems and information, not so much on controlling space or achieving and upholding some kind of superiority over it (Kuehl 2009, 37-38; Nye 2010, 4; Betz & Stevens 2011, 44). At the same time, defense requires constant upgrading, monitoring, and preparations with the view that there is no perfect defense, only resilience (Sheldon 2013, 290-291). *There is no region of cyberspace that is absolutely secure*.

Information societies are dependent on communication and data services. Logistics, finance and critical infrastructure rely on cyberspace. This makes them vulnerable and enticing targets, but state-level attackers are dependent on those same communication and data services, so there is always the possibility of 'mutually assured disruption' (Geers 2011, 121-122). Acting in cyberspace requires recognition and access. Traditionally, the attackers have been considered to have the advantage in cyberspace because every system can be breached given time and the defenders are always reacting. Another way to look at this is, that the development and perhaps the normative costs of attacking and one-time use of weapons is so expensive that the use of cyber weapons may not be efficient (Rid & McBurney 2012; Nye 2016, 71). There is then a logical interest to secure as much of cyberspace under national control as possible. This is of course contrary to the global commons thinking.

If cyberspace gives its own characteristics to the use of power it also affects the threat of use i.e. deterrence. Because there is a problem with attribution, deterring potential attackers is seen to be difficult (Nye 2010, 17). Also, because cyber capabilities are kept secret, it is difficult to convince potential aggressors about the potential to punish or deter them. Be that as it may, there seems to be progress in the ability to transcend the problem of attribution by combining technical forensics, data on earlier incidents, and political context (Nye 2016, 51-52). There have also been cases of shaming and possible multi-spectrum punishment operations against aggressors: for example the United States' operations against North Korea and China (The Washington Post 2014; Reuters 2015; Fireeye 2016). For the time being, the global commons of cyberspace is still a free-for-all environment, including attacks against critical national infrastructure, cf. Prykarpattyaoblenergo, the Democratic National Committee (DNC) hack and WannaCry malware (Fifth Domain, 2017; CNN 2017; The Washington Post 2017).

Based on the description above, we argue that the characteristics of cyberspace seen as a global commons are conducive to symmetry in power. Symmetry rises from the absence of regulative norms, non-transparency, horizontal space, multiple actors, easy access, low costs, and mutual vulnerabilities. In fact, the Internet as a global commons, as an idea and a business model, relies on symmetry. This does not mean that symmetry rules, or that actors strive for it, quite the contrary in fact.

5.2. Asymmetric warfare

Every conflict has asymmetric characteristics (Strachan 2013, 22). There are always vulnerabilities and differences in power. Nevertheless, the concept of 'asymmetric warfare' has appeared and there are universal features how asymmetry is defined in military thinking. Generally, these features relate to unequal military resources and the use of unconventional methods to exploit the vulnerabilities of an adversary.

According to Lawrence Freedman, the idea of asymmetric conflict made its appearance in Western military thinking in the 1970s (Freedman 2006, 52). It was not until the 1990s that asymmetry reached doctrines and

strategies, first as an advantage, but quickly changing to vulnerability as the United States began to confront insurgent forces in intervention operations. During the 1990s and 2000s the thinking on asymmetric warfare intertwined with discourses on the revolution on military affairs, network centric warfare and new generation warfare (Arquilla & Ronfeldt 1997; Cebrowski & Gartska 1998; Owens 2001; Hammes 2006; Chace 2011). Behind all this was a discussion on the changing character of war (van Creveld 1991; Keegan 1993; Kaldor 2012). Basically, asymmetric warfare came to be defined as something done by non-state actors against military superpowers or coalitions that relied on high-tech conventional capabilities and methods, and was restrained by fear of casualties and collateral damage.

There were differences of opinion among what was, basically, a Western community. During the period 1990-2000, there was an argument between the so called Forth Generation Warfare (4GW) thinkers and official network centric warfare proponents. Both tried to legitimize their views on restructuring and re-tasking of modern military forces (Biddle 1998; Evans 2005; Arreguín-Toft 2012; Junio 2015; Echevarria 2017). The idea, that war was somehow changing with the development of information society, and that networked non-state actors were becoming the principal adversaries, clashed with the idea of the triumph of Western military technology and the continuing relevance of conventional military power that was maintained for intrastate war. There was also conflict between the importance of culture and information versus technology. In the writing of 4GW thinkers, asymmetry was not so much a function of power as a function of will, objectives, organization, and norms regulating behavior.

The evolution of U.S. Joint doctrines introduced ideas about multi-spectrum dominance and cross-domain deterrence (Echevarria 2017) which also affected ideas on asymmetry. What these concepts meant from an asymmetrical point of view was that there could be fatal asymmetries in any of the domains of warfare (land, sea, air, space, and cyber) which could be used by an adversary. Already in the 2000s and increasingly in the 2010s military thinkers in the West (and China and Russia) were worried about information as a vulnerability and weapon. It could be used to compel or even to coerce; to win wars without firing a shot by breaking the will of the opponent; to resist or at least paralyze the opponent's military forces. Cyberspace as an infrastructure of information had a prominent role in all of these considerations. (Berkowitz 1997; Freedman 2006; Libicki 2009; Thomas 2015; Nigel 2016; Kaplan 2016.)

The latest incarnation of asymmetry has been the appearance of the so called hybrid warfare. In fact, hybrid warfare has its roots in the same 4GW discussion mentioned above but it was raised to the level of nation states by the illegal annexation of Crimea by the Russian Federation (Hoffman 2009; Renz & Smith 2016; Galeotti 2016). According to earlier versions of hybrid warfare, asymmetry is not seen so much as a type of conflict or difference in power, but as means and methods. Currently, there is a debate going on if, instead of warfare, we should consider hybrid operations as part of political warfare or as some type of next generation warfare (Hoffman 2009; Renz & Smith 2016; Galeotti 2016; Gerasimov 2017). Because of the international political situation, a more traditional approach to asymmetry has also reappeared: it compares specific capabilities in order to find asymmetry (for example missile defense versus Multiple Independently Targetable Reentry Vehicles (MIRVs)). This is reminisced of the Cold War era calculations. (This is closely related to offense – defense theory (Biddle 2001) and evidence of this thinking can be found in Shlapak & Johnson 2016; Heginbotham 2017; and, on the Russian side, see Gerasimov 2017). Cyberspace has a natural place in this kind of thinking as it provides an avenue for messages, pressuring opponents and the limited use of force under the state of war as a part of normal political competition and, if need be, as a part of escalation.

5.3. Asymmetry in cyberspace

Non-state actors have been on the forefront of security studies concerning cyberspace since 1980s (Evolution of the Cyber Domain 2015, 45-47). Discourse on cyber terrorism has been ongoing from the 1990s and has had an effect on national cyber security strategies all over the world (Kaplan 2016; CCD COE 2017). Hackers and criminals have also been seen as a serious security threat for the information society. These threats are by their nature asymmetric. Malign state actors made their appearance in official national security discourse as late as in the late 2000s (Kramer, Starr & Wentz 2009). Not until 2016 was cyberspace designated as a

domain of warfare by NATO (NATO 2016). Therefore, it is not an exaggeration to state that cyber threats have been traditionally seen as non-state and asymmetric.

Asymmetry in cyberspace can be defined with the same pattern as general asymmetric warfare. Cyberattacks are low-cost and low-risk operations that can be launched from a distance with minimal friendly casualties. They can be used by non-state actors against much more powerful state actors and, theoretically, can inflict massive damage on critical infrastructure, loss of life or at least major political fallout. Cyberattacks use vulnerabilities and provide the ultimate battleground for electronic insurgents because the attacker is free to choose when and where to accept combat and can avoid combat altogether if desired. It is difficult to deter a non-state actor or a state actor using a non-state proxy, and what is more disturbing is that common counterinsurgency methods against attackers do not work ('winning hearts and minds'). The problem of attribution is central to asymmetry. If you do not see or know the attacker, you cannot threaten him or strike back (Kramer, Starr & Wentz 2009; Nye 2010, 5).

This traditional concept of asymmetry is tied to a notion of weaker, possibly non-attributable non-state actors using unconventional means as the basis for asymmetric warfare. This, we argue, is too limited a perception of asymmetry in cyberspace. The reason is, firstly, cyberspace is artificial and can be shaped according to security needs of states. Secondly, some states are willing to depart from the idea of the global commons towards the concept of nationally controlled closed networks by delimiting networks, controlling infrastructure, and restricting the flow of information. From one point of view, this aspiration to 'digital sovereignty' can be seen as a legitimate effort to limit and contain asymmetry, rising from the dispersion of power and its perceived vulnerabilities. From a different point of view, this process hides behind the building of a different kind of asymmetry.

We argue that this process creates a new kind of asymmetry, which is based on the shaping of the battlefield space and time. By concentrating on traditional asymmetrical threats in cyberspace, and projects to counter them, we miss the deliberate strategy project of Russia, and some other states, to create asymmetry in the battlefield space and time by digitally and physically controlling certain national and territorial parts of the Internet. Their short-term goals are military and economic; the long-term goals are directed against the so-called Western world order.

5.4. Manipulation of asymmetry

Before we move on to a more detailed analysis of asymmetry in cyberspace as a function of the battlefield space and time, we should take note of how Russians understand asymmetry. As we have argued in chapter 4, Russia is one of the states that are striving for 'digital sovereignty.' The Russian understanding of 'asymmetry' implies an active role in changing the symmetry and creating asymmetry (cf. Thomas 2001, 32). There is a strong connection between non-military and indirect actions, and asymmetrical actions. The idea is to deny the opponent the ability to use force by operating under the level of the open use of force. There should be a continuous search for critical vulnerabilities that might have system-wide effects. By discovering areas where Russia has better combat potential, and thereby using asymmetrical means and methods, a direct military confrontation can be avoided. Information, both its technological and psychological aspect, is seen as a critical aspect of modern warfare. The Russian view is state-centric and based on a perceived technological non-parity with the West (cf. Thomas 2015b, 88, 97, 99, 104).

Alongside the concept of asymmetry, the concept 'initial period of war' has a central place in Russian military thinking. It concerns the first moments of war which might be decisive in modern high-technology warfare against a technologically superior opponent. This concept underlines the preparation of the battlefield and the ability to fight in the whole depth of the battlefield. This means using all the available means in an integrated fashion from the frontlines to the depth of the adversary's home front, and also defending friendly forces, the society, and state from this kind of attack (cf. Thomas 2015b, 231, 233, 244). This could be understood as combining the whole government approach to strategic warfare. Asymmetry in conflict t is then achieved by careful preparation already in the 'gray zone.'

The Russian aim is to reverse the asymmetric advantage[27] it perceives the U.S. enjoys in cyberspace. We argue that in order to gain an asymmetric advantage in cyberspace, Russia is preparing to disconnect the Russian segment of the Internet (RuNet) by 2020. The ambition is to control the Internet routing architecture inside Russia and to maintain operational capabilities outside of the global Internet. This would give Russia a decisive advantage when operating in the 'gray zone' or during the 'initial period of war'. (cf. Ristolainen 2017; Nikkarila & Ristolainen 2017; Kukkola et al. 2017.)

Although, there are many similarities in the Russian concept of asymmetry, it differs from the Western one in a few critical aspects. Firstly, it concerns intrastate competition or warfare. Secondly, it sees asymmetry as something that can be created. Thirdly, it is based on the indirect use of force. And fourthly, it has a role before war is declared, but has the greatest impact during the 'initial period of war'. Based on Russia's drive towards 'digital sovereignty' and the before mentioned differences, we argue that Russia is actively manipulating asymmetry in cyberspace according to its national strategic thinking.

6. ANALYTICAL APPROACH FOR STUDYING CYBER ASYMMETRY

Next, our aim is to broaden the existing traditional strategic, asymmetric, analytical methodologies to cyberspace and to redefine the concept of 'cyber asymmetry'. We argue that future asymmetry in cyberspace is created by shaping the cyber domain, i.e. that the process of closing national networks creates 'cyber asymmetry'.

We argue that 'cyber asymmetry' should be analyzed through factors that we call 'asymmetry factors' in this model. We have deduced these from earlier studies of asymmetry, some of which have been presented in the previous chapter. We are aware that in strategic studies there is a strong critical view on the whole concept of asymmetry. Critics have pointed out that all strategies in all phases of history have tried to achieve asymmetry and find vulnerabilities (Milevski 2014, 79; Strachan 2013, 22). Also, it has been pointed out that asymmetry as an analytical concept has merged with insurgent warfare and nonconventional methods (Arreguín-Toft 2012), and is a culturally a Western concept (Chace 2011). We accept this criticism and try to offer a fresh analytical viewpoint for examining asymmetry in cyberspace.

From previous studies we have deduced at least the following factors concerning asymmetry: Resources (absolute power base), capabilities (relative and contextual power), means (tactics), objectives, will (cost tolerance), norms and culture, organization, information, imagination, space and time (Angström & Widen 2015, 27-30; Freedman 1998, 34; Freedman 2006, 51; Chace 2011, 125; Arreguín-Toft 2012, 636-637; Betz & Stevens 2011, 93; Mitchell 2006; Gartzke & Lindsay 2014; Hammes 2006, 2; Arquilla & Ronfeldt 1997).

The factors we are most interested in are space and time. We are interested in the shaping of cyberspace to achieve asymmetry. Space can be analyzed as distance, borders or environment. In cyberspace, physical distance has little consequences. The digital distance is more important. In this study, we define it as a function of routing (hops, steps, etc.). National or territorial borders have little effect on cyberspace at the moment. Firewalls, filtering, routing, subnetworks and Authentication, Authorization, Audit (AAA) policies have more effect. We are interested in borders because there is a possibility that 'digital sovereignty' will merge territorial and digital borders. The environment is the space where the actors maneuver and act. It consists of geography, roads, weather, and coverage. In the cyberspace environment it depends on the level of analysis. On the physical level it consists of electromagnetic radiation, cables, satellite links, radio connections, routers, and switches. On the syntactic level it consists of networks that are composed of subnetworks, protocols, software, encryption, routes, bandwidth, hosts, services etc. Because cyberspace is partly a non-physical and manmade environment, the norms, rules, and governance are an inherent part of it. They are not scientific laws (i.e. gravity) but changing and open to manipulation. For the above-mentioned

[27] A Russian concept of 'information asymmetry' exists which is one of the core technologies of the Russian 'information counter struggle' (*informatsionnoe protivoborstvo*) (Manoilo 2003, 276). Originally, 'information asymmetry' belongs to economic and contract theory where it is used for creating an imbalance of power in a situation where one party has more or better information than the other. Russian 'information asymmetry' as part of 'information counter struggle' refers to a process where information can be controlled, selected, changed by creating alternative broadcasts, releasing fake news and coverage of events. (Ibid. 278-279.)

reasons, cyberspace is not the same for all or everywhere, and this gives rise to the asymmetrical view of cyberspace.

Time is an important variable because it has a central position in decision-making and in achieving the initiative and attaining surprise. In Western military thinking[28] John Boyd's (1996) Observe-Orient-Decide-Act (OODA) –loop has been used to describe a process whereby faster decision-making can give advantage over an opponent, forcing the opponent into a reactive state and perhaps into total collapse. The OODA Loop is a simplified description of decision-making and it can be argued that it does not capture the processes in complex or novel situations very well and gives undue value to the speed of decision-making. Speed, of course is, not everything; lack of time, bad intelligence, or hasty actions can lead to suboptimal decisions.[29] Nevertheless, there is an important temporal aspect in decision-making. An advantage in decision-making speed might give a belligerent the ability to control the escalation by forcing the opponent to react in a certain way by denying it freedom of action or by threatening important assets. Traditional military thinking also holds that time might be traded for space and vice versa (Hanska 2017, 151-156). How this happens in cyberspace might be studied by investigating the shaping of cyber battlefields.

We do not argue that a battlefield space and time are the only asymmetry variables affecting cyberspace. But because we are interested in the shaping of cyberspace through 'digital sovereignty' and, specifically, in analyzing how this manipulation affects cyberspace as a battlefield, we see space and time as a good starting point for admittedly complex analysis. Our hypothesis is that by creating new frontlines on cyber battlefields, agents can shape the battlefield space and time to their advantage.

The battlefield space and time are not shaped directly or the engagement frontlines created out of thin air. In the cyber domain, the battlefield space and time are affected by technology, norms, governance, and politics. By studying these it is possible to see where, when, and how asymmetry is deliberately or unintentionally created. Because it is difficult, or perhaps impossible, to directly analyze the battlefield space and time as variables of asymmetry, we concentrate our attention on freedom of action, decision-making, and the situation awareness of agents. We consider variation in these three as the product of battlefield space and time related 'cyber asymmetry'. They all are connected to information which permeates cyberspace as a construct, process, and substance. Because freedom of action, decision-making, and situation awareness are information in a sense, we can measure and analyze them as well.

Because we are interested in the 'gray zone' and the 'initial period of war', 'cyber asymmetry' has two important strategic effects. It relates to attribution and escalation. Advantage in attribution gives an agent the ability to direct its use of force more efficiently and to control the conflict militarily and politically. This means that the problem of attribution is turned from a weakness into strength as a characteristic of cyberspace. The advantage in escalation gives the agent the ability to direct the way the conflict evolves, to react more quickly and to threaten the opponent from a position of strength. We analyze these as strategic concepts as outcomes of 'cyber asymmetry'.

In this study we concentrate on the conceptual-technical level and the governance/political level. The conceptual-technical level concerns standards and their theoretical application and the structure of cyberspace. The governance/political level points our attention to shared norms, sovereignty, use of force, security policies, types of government, organization, and the political context of cyberspace. We impose these limitations on ourselves because we are interested in studying how 'digital sovereignty' could be structured (i.e. through BGP and SDN), what kind of policies it requires and how it would affect the future cyber battlefields. We realize that there could be significant technological and practical difficulties in achieving a functioning closed network: it might even lead to catastrophic consequences for the closing nation, but we deem it important to examine the process and consequences nevertheless.

[28] For example: JP 3-0 Joint Operations 17 January 2017.
[29] For an alternative and more comprehensive analysis of decision-making, see for example: Simon 1977, Kulick & Egner 2015.

7. ASYMMETRY IN DIFFERENT TYPES OF BATTLEFIELDS – SPACE AND TIME

Our scenarios start in a situation where Russia declares 'digital sovereignty' and disconnects itself from the global Internet. We argue that in this process cyberspace transforms into different types of subspaces. A subspace is inside the cyberspace, but it has a modified topology within itself and in connection with the other subspaces. Thus, technically at least, it relies on the basic structures of cyberspace when transferring information into and out of other subspaces. In this paper, we have identified three potential types of subspace: 'closed', 'open', and 'fractured'.

The 'closed subspace' is a modified segment of cyberspace where a closed-network nation is technically able to maintain a closed network, i.e. to operate their nationally governed segment of the Internet that can be physically and electronically separated from the global Internet (cf. Kukkola et al. 2017). In the closed subspace category, we separate the primary-closed subspace, i.e. the segment that is disconnected first (Russia) and the closed subspaces that follow the example of the closing process after the primary-closed subspace.

The 'open subspace' is based on the open network. The open network is built upon a society of states. This society is interconnected by a globally accessible network and shares the same basic norms and values concerning information. The open network can be characterized as a global commons. Nevertheless, in this case the 'open subspace' functions without one member present, i.e. the closed-network nation that has disconnected its network from the global system and has started to shape the global cyberspace in order to gain an advantage and control that leads to asymmetry.

The 'fractured subspace' is a modified segment of cyberspace where several of the nations within the open -network society have decided to substantially restrict the information flows and connectivity of their national network[30] (cf. Freedom House 2016; Inkster 2016). In the fractured subspace, individual nations choose their own way to separately react to the network closing processes (cf. secondary-closed subspaces). Some nations might form small alliances, but the general mentality of this subspace is filled with distrust and nervousness. Essentially, a fractured subspace consists of secondary-closed subspaces and the open subspace.

As a result of the process where cyberspace transforms into different types of subspaces, a closed-network nation has managed to shape cyberspace by disconnecting itself from the global Internet. This causes significant structural changes and the division of cyberspace into a mixture of closed and open subspaces that might be followed by further fragmented subspace regiment when the situation develops.

Our scenarios take place in the 'gray zone' of conflict during which the above-defined subspaces clash. Moreover, in this phase the cyberspace transform into a 'cyber domain'. In our lexicon cyberspace is a common platform, whereas 'cyber domain' belongs to the military terminology. When the subspaces come into conflict with each other different types of cyber battlefields emerge. In this paper, we have identified three different types of battlefields which feature a closed subspace[31] in the cyber domain: 1) closed vs. open; 2) closed vs. fractured; and 3) closed vs. closed. These battlefields form scenarios where the battlefield space and time asymmetry variables play an integral and prominent part.

7.1. Closed vs. open battlefield

In our previous studies, we have shown how a closed-network nation (e.g. Russia) has the potential to achieve a significant advantage by following its own strategy (Kukkola et al. 2017). Being a nation that disconnects its networks first from the global network, i.e. the primary-closed subspace, it gains a battlefield advantage over those still trusting/upholding open networks. Russia can control the closed vs. open battlefield with its own concepts that differ significantly from the concepts of nations belonging to an open-network society. Russia's

[30] An example of restricted information flows could serve the Ukrainian block of Russian social media sites (May 2017). This approach promotes an image of a fractured subspace.

[31] Other possible battlefields are: open vs. open, open vs. closed, open vs. fractured, closed vs. closed, closed vs. fractured, and fractured vs. fractured. We recognize that all these battlefields provide interesting scenarios for study. However, we are interest in the ideal type of closed subspace. Therefore, in this paper we do not examine all the possible scenarios.

concepts allow it to operate in the 'gray zone' (cf. 'information counter struggle'). Moreover, a closed subspace is centrally controlled and politically solid, i.e. it is able to make fast decisions[32]. However, the open subspace has the potential to self-organize its administrative structure for common situation awareness, i.e. to form a common understanding of the threats because it can openly share information between different agencies (still, in reality the situation awareness is weak). The closed subspace provides technical solutions for monitoring, restricting, and stopping the incoming traffic better than the open subspace. The 'digital border' between these subspaces is clear. Moreover, the technical solutions maximize situation awareness from a closed-network nation's point of view and it can operate more freely in adversaries' networks than adversaries in its networks. Consequently, the engagement space and time asymmetry variables favor a closed-network nation on a battlefield against an open-network society.

7.2. Closed vs. fractured battlefield

When a primary-closed subspace confronts a fractured subspace, the situation is already more complex because there are multiple secondary-closed subspaces. As the fractured subspace consists of secondary-closed subspaces, the freedom of movement is not as significant as in the previous scenario because there is a multitude of borders. Nevertheless, the technical solutions of a primary-closed subspace allow its agents (at least to some extend) to penetrate and operate in the opposition's secondary-subspace networks. Yet, to operate deeply in those networks is challenging because they might have their own borders and proprietary protocols. However, the space asymmetry does not considerably actualize in the closed vs. open scenario because the administrative structure in the fractured subspace is unclear. On one hand, the unclear organizational structure complicates intelligence missions from the primary-closed subspace point of view. Yet, on the other hand, the unclear administrative structure creates difficulties from the defenders point of view. There is no common situation awareness, i.e. no common understanding of the threats because the information material is not shared between information agencies. Moreover, the fractured subspace regime contains different types of 'digital borders' that may cause difficulties to all of the participants of the conflict, i.e. the problem of attribution is at its worst. Furthermore, the time asymmetry advantage is on the side of the primary-closed subspace.

7.3. Closed vs. closed battlefield

In a battlefield where a primary-closed subspace confronts a secondary-closed subspace, the asymmetry of space is minimal because both sides might deploy the same kind of, but technically different, border procedures and protocols. However, the primary-closed subspace always holds an advantage in time asymmetry because it is technically advanced and politically solid for a certain period of time. The so-called 'asymmetric victory' is gained via the 'information victory' of the primary-closed subspace, i.e. the battle is won without a fight and the world will transform into the so-called 'post-Western world order', where there is nothing left of the cyber commons and 'digital borders' surround every nation-state.

In this chapter, we have analyzed three different scenarios through conceptual technical and governance/political levels and through the battlefield space and time variables. The scenarios of potential future battlefields indicate how asymmetry is created and how it manifests itself. In the following section, we present a predictive model of asymmetric frontlines in a closed vs. open battlefield.

8. ASYMMETRIC FRONTLINES AND FORECASTING MODELLING OF CYBER BATTLEFIELD

In this chapter we focus on the closed vs. open battlefield in more detail as this might be the situation in the near future: because Russia might be actively pursuing this approach and it is also where the 'cyber asymmetry' is most apparently explicit. We use forecasting modelling and explain how asymmetric frontlines are formed in this battlefield. The formation of closed vs. open battlefield is demonstrated in Figure 1. The

[32] Authoritarian leader retains as much power and decision-making authority as possible. Authoritarian leaders make decisions independently with little or no input from other people and therefore the decision-making process is relatively faster than for example in a democratic society (cf. Svolik 2012).

primary-closed subspace is shown encircled on the right, the open subspace is represented as a smaller cloud on the left and the larger cloud containing everything symbolizes the whole cyberspace.

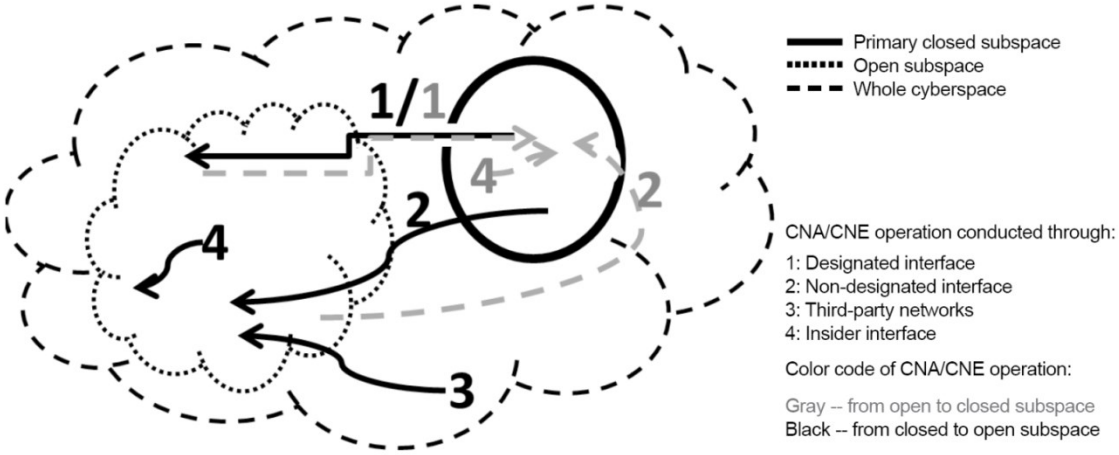

Figure 1. A schematic view of how Computer Network Attack (CNA)/ Computer Network Exploitation (CNE) operations may be conducted from a closed subspace.

In Figure 1, the arrows illustrate possible Computer Network Attack (CAN)/ Computer Network Exploitation (CNE) operations. The closed subspace is shown encircled, the smaller cloud represents the open subspace and the larger cloud represents the whole cyberspace. Operations from the primary-closed subspace into the open subspace are illustrated as a solid line and operations in the opposite direction are shown as a dashed line. Next, we categorize operations and list and analyze their properties to resolve if asymmetry is present in the new circumstances. The operation categories are: 1) through the designated interface[33]; 2) through non-designated interface; 3) through third party networks; 4) insider interface. In the following sub-chapters we will explain all of the operation categories. First, we examine the effects on the close subspace's defense and second, we study the effects to the closed subspace's offense.

8.1. Designated interface

There are the following effects on the closed subspace's defense: the designated interface is likely to be well-protected and monitored, especially in the direction of the closed subspace. An operation from an open subspace into the closed subspace through this interface is not preferable as the connection may be monitored, controlled, and even blocked when necessary. Even the blocking of all of the traffic can be justified as a non-aggressive and defensive action. The possible requirement of an agent or a responsible party for all the traffic into a closed network means that offensive operations will be more difficult. At the minimum, the first indications of harmful traffic are at hand almost immediately when it is detected in a closed subspace. If registration at the 'digital customs' is required (cf. Streltsov & Pilyugin 2016, 28-29) the problem of attribution is diminished. However, the problem of attribution is not entirely solved if the attacker uses third party networks in order to conduct its operation and the registrant is an intermediate victim. Nevertheless, the closed-network nation may trace the attack back to the first step outside its own network e.g. to a liable partner that has agreed to the required conditions. The designated interface provides an undisputable advantage in situation awareness to the closed-subspace defender and, along with centralized monitoring and controlling, enhances decision-making (cf. Svolik 2012).

The effects on the closed subspace's offense are the following: An operation conducted from the closed subspace into the open subspace may not currently be controlled as extensively as into the opposite direction. For instance, the origin of the traffic may be hidden almost immediately after crossing the border, for example with IP-hiding services. Even if the monitoring is successful, there are no current methods to prevent such harmful services' actions. The closed-subspace attacker may take advantage of the target nation's information technology infrastructure in its offense and use the designated interface only to deliver the most important commands, thus limiting situation awareness on the open subspace side. If all of the outgoing connections to the open subspace from the closed subspace are disconnected by the open-subspace

[33] A designated interface is, for example, a nationally controlled IPX that has an open interface to ingress / egress traffic to outside networks.

agent, the closed-subspace actor could see the action as aggressive or even comparable to an armed attack. Nevertheless, the designated interface limits the freedom of action of a closed-subspace attacker. There is at least a theoretical possibility to be caught and more importantly, the operation may be suspended if the open subspace blocks the traffic from the closed subspace. The open-subspace defender has a limited situation awareness and faces the attribution problem. This gives the attacker an advantage in time.

As a result, even if all of the operations go through the designated interface, the differences in situation awareness and the effectiveness of decision show that there is an asymmetry in both the battlefield space and time.

8.2. Non-designated interface

The effects on the closed subspace's defense are the following: The open subspace attacker has to perform additional measures, for example reconnaissance, in order to penetrate into the system. In practice, first the attacker has to find and reconnoiter the interface for the attack. Second, even if the penetration is successful, the legitimacy of the traffic is likely to be checked in every router. Therefore, the attacker has to conduct deceptive actions in order to be able to penetrate into, and to operate within, the closed network. The attack may be disrupted before the actual target and the traffic may be forwarded into the border and/or the incident may be handled as an unauthorized border crossing. The attempt may be considered to be a military action with adequate consequences. Moreover, because the attacker's traffic is unauthorized, it might have problems with protocols, encryption, authentication, and software compatibility. Even if the propagation is successful, there would not necessarily be a control connection available. Therefore, even if a non-designated interface is used, the defender has better situation awareness, decision-making capabilities, and the freedom of action in its own networks.

Effects to the closed subspace's offense are the following: By its definition, the operation is conducted from inside the closed subspace and the primary reason for this would be the straightforwardness of the command line and the execution of the operation. The operation personnel work within the closed subspace's geographical location and the freedom of movement is high. 'Contiguous systems' – yet topologically detached from the closed subspace – may be used for offensive operations through a non-designated interface within the closed subspace. The 'contiguous systems' would likely be separated in both the administrative sense and topologically from the rest of the network. Furthermore, the systems would likely take advantage of the basic structures of cyberspace whenever it is possible. The reason for using the parallel systems could be to hide the origin of the operation. The defender in the open subspace has a full attribution problem, as finding the agent responsible for the assault is both difficult and time consuming. Since this non-designated interface 'does not exist', it creates an additional non-regulated attack vector which may be difficult to analyze and resolve. Because of these restrictions on the open-subspace defender's situation awareness, an attacker may conduct a surprise attack that is difficult to monitor and attribute. A particular challenge is that the execution of the operation requires additional set ups such as the contiguous systems, which might be detected by means outside of cyberspace.

As a result, the use of non-designated interfaces reveals a significant asymmetry between the closed and open subspaces. The asymmetry is mainly expressed through freedom of action and better situation awareness. It is important to note that the majority of the barriers or blockades within the closed subspace do not exist in an open subspace.

8.3. Third party networks

Effects on the closed subspace's defense are the following: This method is considered implicitly in subchapters 8.1. and 8.2 and consequently is a combination of the methods mentioned therein. When an open subspace attacker uses third party networks for its operation, it is likely to use a non-designated interface. In that case, most of its challenges are mainly related to the penetration and propagation in the defender's systems. On the other hand, one may use a designated interface, but it is likely that this is addressed in any agreements between the closed subspace and 'third party networks' if they exist.

Effects to the closed-network subspace's offense are the following: Offensive operations conducted via 'third party networks' provide even more freedom of action than operations conducted through a non-designated interface. The only drawback is that the operation personnel may have to work in a third party state as well. Yet, one is able to use existing infrastructure in order to conduct the operation. From the defender's perspective, the problem of attribution may be even higher than in the previous cases. Probably one is able to find out the actual origin (state) of the assault only if the personnel are caught. Otherwise, the signs of the true origin are likely to be masked as 'cybercriminal' or 'hacktivist' activity. The attacker may conduct its operation from an allied country in order to further complicate the investigation. As in subchapter 8.2., the attacker may conduct a surprise attack and it is almost impossible for the defender to monitor all of the networks of cyberspace. Moreover, closed-subspace operations are possible even if it is disconnected from the global network. The same might not be true with open subspace attackers.

As a result, using 'third party networks' provides such as a freedom of action to the closed subspace attacker that asymmetry in the battlefield space and time is considerable.

8.4. Insider interface (requires physical presence in the target country)

Effects to the closed subspace's defense are the following: When building up its defense, a closed subspace is likely to benefit from central control and solid authoritarian politics. Consequently, the attacker may encounter difficulties in infiltrating its personnel into the target region. They may also have to deal with local software and hardware. On the other hand, from the attacker's perspective one may solve the majority of the problems related to penetrating and propagating the defender's systems given enough time for reconnaissance. The defender can frame the issue legally and politically as an aggressive action, even as an act of war. The defender may consider the attackers as conducting a high-risk Special Operations Force (SOF) mission. In the case of an insider threat, the closed-subspace defender's situation awareness is restricted because the system treats the attacker as a legitimate user. The closed-subspace actor's networks are compromised because 'security through obscurity' has been proved faulty. Nevertheless, an authoritarian system enables defender to react quickly and comprehensively if its networks are compromised. And the drawback of the authoritarian system is that it requires societal control, including comprehensive monitoring of its own citizens. During the past years, Russia has intensively ratified new laws[34] for surveillance and control that can be seen as an attempt to solve this challenge (cf. Ristolainen 2017).

Effects to the closed subspace's offense are the following: The information of open-subspace critical systems are either openly available or, at least, can be reconnoitered via the Internet. The information consists of physical properties, such as location, the location and types of interfaces, or operation systems' models and versions etc. The corresponding system vulnerabilities are openly downloadable via the Internet. In addition, it is relatively easy to physically reconnoiter interesting locations. It might not even be illegal to some extent. Then again, this method may be the only method where the defender has the authority to verify the incident and is able to sanction the suspects. The defender still has an attribution problem, but it may not be as substantial. Finally, from the attackers' perspective this method is a preferable option only if the previous three methods are not possible.

As a result, in this method the asymmetry is at its lowest level. The battlefield space and time equally affect both belligerents. Still, the differences in the openness of societies that affect the situation awareness give a decisive advantage to the closed-subspace attacker.

[34] These laws allow, for instance, *Roskomnadzor* (the Federal Service for Supervision of Communications, Information Technology and Mass Media) to block and to censor harmful information and websites deemed extremist or a threat to public order; demand the owners and operators of websites to store all information about the arrival, transmission, delivery, and processing of voice data, written text, images, sounds, or other kinds of action and to keep this content for six months; limit anonymous money transfers and donations on the internet; require all web-based writers (bloggers, social media accounts) with posts that exceed 3000 page views to register with the government; dissemination or re-dissemination (tweeting and retweeting) of 'extremist materials'; require internet companies, including Google, Twitter, and Facebook, to locate servers handling Russian internet traffic inside the country and to store their users' data on these locally-based servers for a minimum of six months; to prohibit anonymous access to the Internet in public spaces; hold media, news services and search engines liable for all the content in their publications (e.g. linking reposting, and automatically-created links); forbid owners of virtual private network (VPN) services and Internet anonymizers from providing access to websites banned in Russia (cf. Ristolainen 2017).

8.5. Asymmetric frontlines

As we have shown in subchapters 8.2-8.4, 'cyber asymmetry' manifests most clearly when an open-subspace attacker tries to penetrate into a closed subspace. We will analyze this issue in more detail in the figure below. We argue that the closed subspace can succeed in constructing additional frontlines within its own subspace. The frontlines of a closed subspace are illustrated in Figure 2. The routers are marked with the letter R with a lowering index. For example, BGP refers to the border gateway protocol and SDN to software-defined networking (the routing decisions are conducted at R_{SDN}). The traffic from the border to the target (T) is demonstrated with a dashed line. The ordering of the routers in the mentioned path is represented by router lowering index numbers. The SDN controlled connection between the routers and the SDN control unit (R_{SDN}) is shown as a dotted line. It is important to note that there can be several control units R_{SDN1}, R_{SDN2} etc., and that they may be located differently than shown in Figure 2.

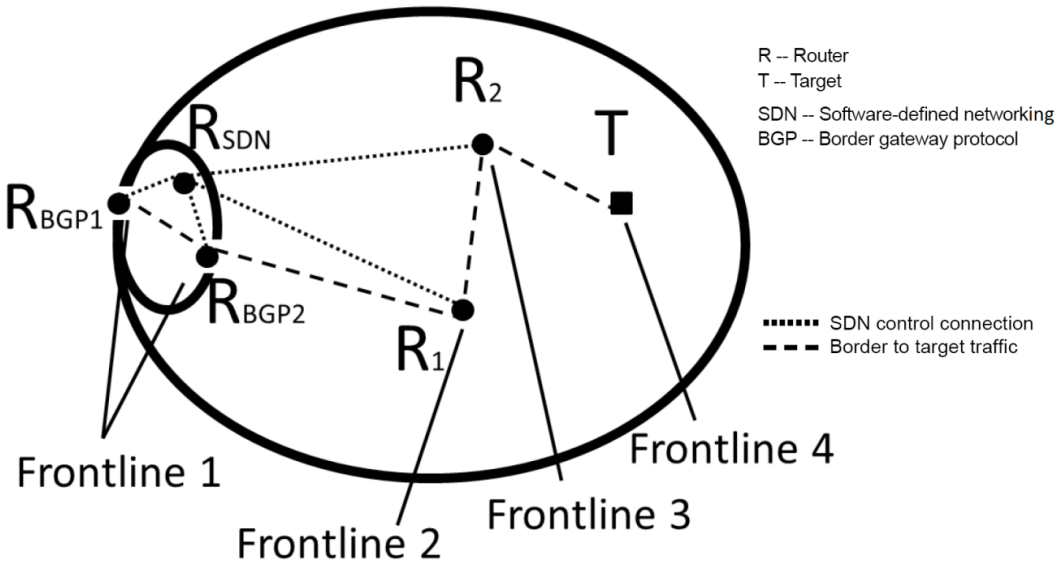

Figure 2. A simplified schematic outline of the frontlines of a closed subspace. The largest ellipse represents the closed subspace and the smaller demonstrates the 'border crossing-point' and 'digital customs' (cf. Streltsov & Pilyugin 2016) between the open subspace and the closed subspace. It needs to be noted that in practice the closed subspace is further divided into several autonomous systems. In the Figure one, the decision-making router R_{SDN} is actually a set of several routers that may be centrally controlled. This kind of administrative structure likely requires the most significant development and resources.

When an attacker is attacking the target, it faces several challenges on the way before reaching the target itself. The first challenge is at the 'digital border' where the connection author has to register. The source of the connection is verified to be a legitimate source. From the attacker's perspective this is **the first frontline**. Usually, it would not be reasonable to conduct an attack in your own name unless you wanted to perform a show of force. Requiring registration provides additional asymmetry that affects all of the frontlines and it may also have an impact on the political level. The registration can be seen as an attempt to remove or at least to diminish the problem of attribution described in 8.1-8.4. **The second frontline** is at the first router on the path to the target. At the router one can check if the source IP address is a legitimate source, even if the destination IP is permissible, and if the 'digital border crossing' has been authorized, etc. At the second router everything is done again and on top of that one might even check if the route of the connection has been appropriate (**the third frontline**). Consequently, an additional frontline is formed at every router bringing asymmetry into space. The routing tables can be updated straightforwardly and quickly when required, which provides time asymmetry as well. As a result, the attacker has to develop methods to circumvent these frontlines in order to maintain its operational capability.

If the connection to the target is successful, the remaining challenges are related to that IT system's own defensive measures such as firewalls (**the forth frontline**). An additional feature is that the hardware and the software may be different than what used in the open subspace. The difference is mainly a challenge, but on the other hand it may be an opportunity as they will likely have different types of vulnerabilities. The systems

of a closed subspace are not threatened by similar types of constant attacks as open networks' operation systems. Therefore, their development may not be as fast and extensive as in the open networks. Finding the vulnerabilities requires syntax understanding and constant learning. As a result, the battlefield space and time asymmetry is formed by the systems' own defensive measures, but the resulting asymmetry does not benefit the closed subspace as drastically as the other frontlines. In other words, an open subspace needs to reconnoiter more and expend more effort in order to maintain its operational capabilities. In addition to the described frontlines, with the help of SDN the traffic can be directed to a honeycomb or a honeypot network on the fly, based on the reliability of the source (cf. Dutta 2016).

What makes the frontlines described above asymmetric is that they exist only for one of the belligerents in a potential conflict. An open-network actor's freedom of action, situation awareness, and decision-making are hampered when it conducts offensive operations. On the contrary, the closed-network attacker can operate quite freely in the depth of an open network. Moreover, it confronts frontlines only at the target, if even then. This is the core of the battlefield space and time-based cyber asymmetry.

In our analysis we have shown that the frontlines of a closed network; the possibility to completely disconnect a closed network from other networks; and, the relative freedom of action in open-society networks create a 'cyber asymmetry' that favors a closed-network nation. It has greater situation awareness, a faster decision-making cycle, and more freedom to maneuver than states with an open-network society. It can attack wherever and whenever it wants. It has the advantage in attribution and the ability to control escalation. All this can be achieved already in the 'gray zone', and if a political competition escalates into an open conflict. It will also potentially provide an initiative in cyberspace. This finding corresponds with our earlier studies. (Kukkola et al. 2017.)

9. RESULTS: CYBER ASYMMETRY AND THE BATTLEFIELD OF THE FUTURE

The aim of this paper was to consider what a future cyber battlefield could look like. Our paper was divided into conceptual and practical parts that reflect the objective from different perspectives. We have explained how the Russian ambition to 'digital sovereignty' belongs to the framework of state security, and how the external aspect of this project is to challenge the Western world order. Moreover, we argue that the military aim of this Russian project is to gain an advantage and to form an imminent 'cyber asymmetry' that expertly influences future cyber battlefields. The technical solutions in our study were restricted to an existing BGP protocol combined with the SDN networking architecture as a probable technical solution behind the closed national network.

We claimed that the conventional understanding of asymmetry in cyberspace based on the problem of attribution is too limited. We reinforced this argument by explaining the characteristics of cyberspace in relation to asymmetry as a military theoretical concept. Cyberspace is artificial and can be shaped which is at the core of a process where a new kind of 'cyber asymmetry' is created. We argued that by concentrating on traditional asymmetrical threats in cyberspace we miss a deliberate strategy by Russia (and some other states) to manipulate asymmetry digitally and by physically controlling certain national and territorial parts of the open Internet.

We produced an analytical approach for comparative analysis of asymmetry in cyberspace. Our analysis demonstrated how the battlefield space and time variables form a base for asymmetry on the future cyber battlefield. By studying on the one hand the creation of asymmetry and on the other its effects on the freedom of action, decision-making, and situation awareness of belligerents, we could analyze the creation and dynamics of 'cyber asymmetry'. The battlefield space and time variables were observed through changes in these three phenomena.

We presented a scenario where Russia declares 'digital sovereignty' and disconnects itself from the global Internet. We argued that in this process cyberspace could transform into different types of subspaces that are 'closed', 'open', and 'fractured'. The structural changes in cyberspace could increase the probability for a nation state confrontation. When the subspaces collide, different types of cyber battlefields emerge. We

analyzed asymmetry through the battlefield space and time variables in different types of battlefield scenarios and showed that belligerents can shape the battlefield space and time to their advantage.

Finally, we focused on the closed vs. open battlefield in more detail as this might be the near future situation and also where 'cyber asymmetry' is most explicit. We categorized different CNA/CNE operations and listed their properties and analyzed what effect they have on the closed subspace's defense and offense. Furthermore, we used forecasting modelling when explaining how a closed subspace can succeed in constructing asymmetric frontlines within its own subspace.

According to our analysis, the future cyber battlefield might be characterized by a new kind of asymmetry, where resources and methods give way to the ability to shape the battlefield space. The frontlines that are different for the belligerents become the source of asymmetry. By creating multiple frontlines in depth based on national control of the Internet, a belligerent can achieve an asymmetric advantage. This advantage can be used in a 'gray zone' and the initial period of war to operate more freely; to lessen the problem of attribution (thereby increasing deterrence) and to control escalation by threatening an opponent with disruption and its diminished possibility for a counter strike.

10. DISCUSSION AND RECOMMENDATIONS

There is a tendency in Russian foreign policy and security establishments to view Russia as being surrounded by enemies and historically defending itself against outside threats (Aron 2008; Blank 2008; Monaghan 2008). There is also a school among Western analysts that sees Russia as a defensive great power (Mearsheimer 2014, Sakwa 2015, Walt 2015). At first glance, our findings seem to support these claims. Russia, through 'digital sovereignty', is building a strong and resilient cyber defense through a closed subspace. But, as we have shown, in 'cyber asymmetry' there is also an inherent advantage to a closed subspace attacker.

In 1725 French engineer Philippe Maigret wrote that: "the best kind of fortresses are those that forbid access to one's country while at the same time giving an opportunity to attack the enemy in his own territory." (Guerlac 1990, 87). Asymmetric frontlines in cyberspace might not resemble 18th century fortresses but there is a similar logic behind them: Deny and Enable. This digital fortress built on principles of self-sufficiency and deep defense, is constructed during peace time and in a 'gray zone' and during the initial phase of a war the asymmetry it creates makes the so called 'reactive action' or 'active defense' of opponents difficult, or even impossible, to conduct while at the same time enabling offensive cyber operations in the depth of the enemy 'territory'. If need be, all connections into the cyber/digital fortress can be disconnected and still the digital fortress / agent can support missions outside its 'walls'.

Even if historical comparisons might be somewhat arbitrary, the 'cyber asymmetry' we have described in this paper is real. If Russia chooses to pursue the idea of 'digital sovereignty' to its logical end and if it manages to persuade others to follow it, the values and security of the open-network society, based on free, open and secure cyberspace might be in danger. Without a collective approach to this threat, the nations of the open-network society can only close their own national networks. Needless to say, this will make small nations vulnerable, lead to economic problems by destabilizing the global digital economy, erode Western values for the benefit of authoritarian tendencies, and destroy the Internet as we know it.

How then, can the open-network society manage the asymmetry created by closed-network nation(s) without sacrificing its core values? It can start by strengthening the resilience of the open networks and at the same time by studying the vulnerabilities of closed networks to deter those nations from planning to close their networks and thus to keep them open. The open-network society has to prepare for an asymmetric conflict on cyber battlefields if deterrence fails. Taking the easy way and abandoning the open-network society could not provide a military advantage and would truly lead to a post-Western world order. It is tantamount to surrender. The understanding of the cyber battlefields requires a multidisciplinary approach involving all levels of decision-making from the technical to the political and all branches of government. This is not something that individual nations can achieve by themselves. It has to be a collective endeavor.

REFERENCES

Angström, J. & Widen J.J. (2015): *Contemporary Military Theory: The Dynamics of War*, Routledge: New York.

Aron, L. (2008): The Problematic Pages, *New Republic*, September 24, 2008, https://newrepublic.com/article/62070/the-problematic-pages (Accessed 6 June 2017).

Arreguín-Toft, I. (2012): Contemporary Asymmetric Conflict Theory in Historical Perspective, *Terrorism and Political Violence*, 24:4, 635-657.

Arquilla, J. & Ronfeldt, D. (1997): *In Athena's Camp*, RAND: Santa Monica.

Ashmanov, I. (2013): *Doklad: Informatsionnyi suverenitet. Sovremennaia real'nost',* [Presentation: Information Sovereignty. Contemporary Reality], 24 April 2013, http://rossiyanavsegda.ru/read/948/ (Accessed 17 October 2016).

Bakharev N.F., Polezhaev P.N., Suchman, A.E. & Ushakov Yu.A. (2015): Upravlenie korporativnymi programmno-konfiguriruemymi setiami [The management of corporate software-configurable networks], *Vestnik Orenburgskogo gosudartsvennogo universiteta* 13(188), 108-113.

Barlow, J. (1996): *A Declaration of the Independence of Cyberspace*, https://www.eff.org/cyberspace-independence (Accessed 3 June 2017).

Barno, D. & Bensahel, N. (2015): *Fighting and Winning in the "Gray Zone"* (May 15, 2015), https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/ (Accessed 15 May 2017).

Berkowitz, B.D. (1997): Chapter seven: Warfare in the Information Age. Arquilla, J. Ronfeldt, D. (eds.), *In Athena's Camp*, RAND: Santa Monica, 175-189.

Betz, D.J. & Stevens, T. (2011): *Cyberspace and the State: Toward a Strategy for Cyberpower*, Adelphi Series 51:424.

Biddle, S. (1998): The Past as a Prologue: Assessing theories of future warfare, *Security Studies*, 8 (1), 1-74.

Blank, S. (2008): Threats to and from Russia: An Assessment, *The Journal of Slavic Military Studies*, 21 (3), 491-526.

Boyd, J. (1996): *The Essence of Winning and Losing*, https://fasttransients.files.wordpress.com/2010/03/essence_of_winning_losing.pdf (Accessed 3 June 2017).

Carr, J. (2012): *Inside Cyber Warfare*, O'Reilly: Sebastopol.

CCD COE (2017): *Cyber Security Strategy Documents*, https://ccdcoe.org/cyber-security-strategy-documents.html (Accessed June 12th 2017).

CNN (2017): *Intel report: Putin directly ordered effort to influence election*, http://edition.cnn.com/2017/01/06/politics/intelligence-report-putin-election/index.html (Accessed 3 June 2017).

Cebrowski A.K. & Gartska J.J. (1998): *Network-Centric Warfare: Its Origin and Future*, http://www.kinection.com/ncoic/ncw_origin_future.pdf (Accessed 3 June 2017).

Chace, J.G. (2011): Defining Asymmetric Warfare: A Losing Proposition, *JFQ*, 61, 123-126.

Chalyy, D.J., Nikitin, E.S., & Antoshina, E.J. (2015): A simple Information Flow Security Model for Software-Define Networks. *Proceedings of the 17th Conference of Open Innovations Association FRUCT*, Yaroslavl, Russia, 276-282.

Chemeritskii, E.V. (2015): Issledovanie metodov kontrolia funktsionirovaniia programmno-konfiguriruemykh setei [A study of control methods for monitoring Software-Defined Networks], *PhD-Dissertation*, Moscow State University, Moscow.

Chouri, N. (2012): *Cyberpolitics in International Relations*, MIT Press: Cambridge.

Cisco (2016): *Block One or More Networks from a BGP Peer*, http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13750-22.html (Accessed 7 June 2017).

Coates, J. F. & Glenn, J. C. (2005): "Normative forecasting," in The millennium project, futures research methodology – V2.0 , J. F. Coates and J. C. Glenn (eds.), *AC/UNU Millennium Project*.

Critical Terminology Foundations 2 (2014): *Critical Terminology Foundations 2. Russia-U.S. Bilateral on Cybersecurity.* Policy Report 2/2014, Godwin III, J.B., Kulpim, A., Rauscher, K.F. & Yaschenko, V. (eds.), EastWest Institute and the Information Security Institute of Moscow State University.

Van Creveld, M. (1991): *The Transformation of War*, The Free Press: New York.

CyCon (2016): *8th International Conference on Cyber Conflict (CyCon 2016): Cyber Power*, Proceedings. Pissanidis, N., Rõigas H. & Veenendaal, M. (eds.), https://ccdcoe.org/cycon/2016/proceedings/CyCon_2016_book.pdf (Accessed 6 June 2017).

DATAIX (2017): *Homepage*, http://dataix.ru/partnership/ (Accessed June 9th 2017).

Demchak, C. & Dombrowski, P. (2013): Cyber Westphalia: Asserting State Prerogatives in Cyberspace, *Georgetown Journal of International Affairs*, vol. International Engagement on Cyber III, 29-38.

Doktrina (2016): *Dokrina informatsionnoi bezopasnosti Rossiiskoi Federatsii* [Information Security Doctrine of the Russian Federation], December 5, 2016, http://static.kremlin.ru/media/acts/files/0001201612060002.pdf (Accessed 5 May, 2017).

Draft (2017): *United Nations Convention on Cooperation in Combating Information Crimes* – an unofficial draft that Russia has presented and distributed for discussion in Commission on Crime Prevention and Criminal Justice, UN. (22-26 May 2017).

Dubov, D.V. (2014): Kibermogushchestvo kak bazis obespecheniia ”tsifrovogo” suvereniteta v sovremennom mire: kliuchevie podkhody. [Cyberpower as a fundamental concept for “digital” sovereignty in the contemporary world: Key aspects], *Oborona i bezopasnost'*, 4 (25), 123-135.

Dutta, M. (2016): A Review of Automated Intrusion Detection Models, *International Research Journal of Engineering and Technology (IRJET)*, 3 (5), 1980-1983.

Echevarria, A. (2017): *Operational Concepts and Military Strength, 2017 Index of U.S. Military Strength*, http://index.heritage.org/military/2017/essays/operational-concepts-military-strength/ (Accessed 15 March 2017).

Ermoshina, K. & Musiani, F. (2017): Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era, *Media and Communication*, 5 (1), 42-53.

Evans, M. (2005): Elegant irrelevance revisited: A critique of fourth-generation warfare, *Contemporary Security Policy*, 26:2, 242-249.

Evolution of the Cyber Domain (2015): *Evolution of the Cyber Domain: The Implications for National and Global Security*, Tikk-Ringas, E. (ed.), The International Institute for Strategic Studies, Routledge: London.

Federal'nyi zakon (2017): *O sviazi, 07.07.2003, No. 126-FZ (poslednaia redaktsiia ot 17.04.2017, No. 75-FZ),* [Federal Law On connections 07.07.2003, No. 126-FZ (last updated 17.04.2017, No. 75-FZ)], http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=215565&fld=134&dst=1000000001,0&rnd=0.425694509185802#0 (Accessed June 9th 2017).

Fifth Domain (2017): *Hackers' methods feel familiar in Ukraine power grid cyberattack*, http://fifthdomain.com/2017/01/29/how-a-power-grid-got-hacked/ (Accessed 3 June 2017).

Fireeye (2016): *Redline Drawn: China Recalculates Its Use of Cyber Espionage,* https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf (Accessed 3 June 2017).

Freedman, L. (1998): *Asymmetric Wars*, Adelphi Papers, 38:318, 33-48.

Freedman, L. (2006): *The Revolution in Strategic Affairs*, The Adelphi Papers, 45:379.

Freedom House (2016): *Freedom on the Net 2016 report* (November 2016), https://freedomhouse.org/sites/default/files/FOTN_2016_Full_Report.pdf (Accessed 24 May 2017).

Gartzke, E. & Lindsay, J. (2014): *Cross-Domain Deterrence: Strategy in an Era of Complexity*, https://quote.ucsd.edu/deterrence/files/2014/12/EGLindsay_CDDOverview_20140715.pdf (Accessed 3 June 2017).

Geers, K. (2011): *Strategic Cyber Security*, NATO CCD COE: Tallinn.

Gerasimov, V. (2017): *Vystuplenie nachal'nika Genshtaba VS RF generala armii Valeriia Gerasimova na konferentsii MCIS-2016* [The speech of the chief of the General staff of the Russian Armed Forces General Valery Gerasimov at the conference MCIS-2016], http://mil.ru/mcis/news/more.htm?id=12120704@cmsArticle (Accessed 8 June 2017).

Guerlac, H. (1990): Vauban: The Impact of Science of War, *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, Paret, P.(ed.), Clarendon Press: Oxford, 64-90.

Hammes, T.X. (2006): *The Sling and the Stone: On War in the 21st Century*, Zenith Press: St Paul.

Hanska, J. (2017): *Times of War and War over Time: The roles time and timing play in operational art and its development according to the texts of renowned theorists and practitioners*, National Defence University: Helsinki.

Heginbotham, Eric (ed.) (2017): *The U.S. - China Military Scorecard: Forces, Geography, and the Evolution of Balance of Power 1996-2017*, RAND: Santa Monica.

Hoffman, F.G. (2009): Hybrid warfare and challenges, *JFQ*, 52, 1st quarter, 34-39.

ICANN (2017): *The problem with 'seven keys'*, https://www.icann.org/news/blog/the-problem-with-the-seven-keys (Accessed 7 June 2017).

Inkster, N. (2016): *China's Cyber Power*, Routledge: New York.

Internet Live Stats (2017): *Russia Internet Users*, http://www.internetlivestats.com/internet-users/russia/ (Accessed 9 June 2016).

Izvestia.ru (2016): *V Rossii poiavilsia voennyi internet* [A military internet appeared in Russia], 19.10.2016, http://iz.ru/news/639221 (Accessed 9 June 2017).

Junio, T.J. (2012): Military History and Fourth Generation Warfare, *Journal of Strategic Studies*, 32:2, 243-269.

JP 3-0 Joint Operations (2017): *JP 3-0 Joint Operations*, 17 January 2017, IV-2 http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf (Accessed 13 June 2017).

Kaldor, M. (2012): *New and Old Wars: Organized Violence in a Global Era*, Stanford University Press: Stanford.

Kaplan, F. (2016): *Dark Territory. The Secret History of Cyber War*, Simon & Schuster: New York.

Keegan, J. (1993): *A History of Warfare*, Vintage Books: New York.

Konstantinov I.S., Chashin J.G. & Lazarev S.A. (2014): Simulation of the Software-Defined Network for a High-Performance Computing Cluster, *Research Journal of Applied Sciences* 9 (10), 704-706.

Kosow, H. & Gaßner, H. (2008): *Methods of Future and Scenario Analysis: Overview, Assessment, and Selection Criteria*, German Development Institute: Bonn.

Kramer, F.D., Starr, S.H. & Wentz, L.K. (2009): *Cyberpower and National Security*, National Defense, University Press: Washington D.C.

Krasotin, A.A. & Alekseev, I.V. (2013): Programmno-konfiguriruemye seti kak evoliutsii setevikh tekhnologii [Software-Defined Networks as a Stage of the Network Technology Evolution], *Modelirovanie i analiz informatsionnykh sistem*, 20 (4), 110-124.

Kreutz D., Ramos F.M.V, Veríssimo P.E., Rothenberg C.E., Azodolmolky S. & Uhlig S. (2015): Software-Defined Networking: A Comprehensive Survey, *Proceedings of the IEEE*, 103 (1).

Kucheriavyi, M.M. (2014): *Informatsionnye izmerenie politiki natsional'noi bezopasnosti Rossii v usloviiakh sovremennogo globalnogo mira* [Information Dimensions of the Russian National Security Policy in the Modern Global World]. PhD-Dissertation, Saint Petersburg State University: St. Petersburg.

Kuehl, D.T. (2009): From Cyberspace to Cyberpower - Defining the Problem. Kramer, F. D., Starr, S. H. & Wentz, L.K. (eds.), *Cyberpower and National Security*, National Defense University Press: Washington D.C., 24-42.

Kukkola, J., Ristolainen, M. & Nikkarila, J-P. (2017): Confrontation with Closed Network Nation: Open Network Society's Choices and Consequences, forthcoming in *MILCOM 2017*: Baltimore.

Kulick, D.P, & Egner, M. (2015): *Implications of Modern Decision Science on Military Decision Support Systems*, RAND: Santa Monica.

Lango, H-I. (2016): Competing academic approaches to cyber security. *Conflict in Cyber Space: Theoretical, strategic and legal perspectives.* Friis, K. & Ringsmose, J. (eds.), Routledge: New York, 7-26.

Lavrov, S. (2017): *Foreign Minister Sergey Lavrov's address and answers to questions at the 53rd Munich Security Conference, Munich, February 18, 2017*, http://www.mid.ru/en/foreign_policy/news//asset_publisher/cKNonkJE02Bw/content/id/2648249 (Accessed 19 March 2017).

Libicki, M.C. (2009): *Cyberdeterrence and Cyberwar*. RAND: Santa Monica.

Manoilo, A.V. (2003): *Gosudarstvennaia informatsionnaia politika v osobykh usloviiakh* [State Information Policy in Special Circumstances], MIFI: Moscow.

Martino, J. P. (1993): A comparison of two composite measures of technology, *Technological Forecasting and Social Change*, 44, 147-159.

McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., & Turner, J. (2008): OpenFlow: Enabling Innovation in Campus Networks, *Computer Communication Review*, 38 (2), April 2008, 69-74.

Mearsheimer, J. (2014): *Getting Ukraine Wrong,* https://www.nytimes.com/2014/03/14/opinion/getting-ukraine-wrong.html?_r=0) (Accessed June 6, 2017).

Milevski, L. (2014): Asymmetry is Strategy, Strategy is Assymmetry, Joint Force Quarterly, 75(4) October 1, 77-83

Minkomsvyaz (2016): *Federal'nyi zakon "O vnesenii izmenenii v Federal'nyi zakon "O sviazi" (Proekt)* [Federal Law "On the changes to the Federal Law "On connections"], October 2011, 2016, http://regulation.gov.ru/projects#npa=58851 (Accessed 22 October 2016).

Mitchell, P.T. (2006): *Network Centric Warfare: Coalition operations in the age of US military primacy*, IISS, The Adelphi Papers, 46:385.

Monaghan, A. (2008): 'An enemy at the gates' of 'from victory to victory'? *Russian foreign policy, International Affairs*, 84 (4), 717-733.

MSK-IX (2017): *Homepage*, https://www.msk-ix.ru/company/ (Accessed June 9th 2017).

Muller, L. (2016): How to govern cyber security? The limits of the multi-stakeholder approach and the need to rethink public-private cooperation. *Conflict in Cyber Space. Theoretical, strategic and legal perspectives*. Friis, K. & Ringsmose, J. (eds.) Routledge: New York, 116-129.

NATO (2013): *Comprehensive Operations Planning Directive COPD V2.0*, 04 October 2013. www.act.nato.int/images/stories/events/2014/sfpdpe/copd_v20.pdf. (Accessed 20 March 2017).

NATO (2016): *Warsaw Summit Communiqué*, http://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber (Accessed 3 June 2017).

Nikkarila, J-P. & Ristolainen, M. (2017): 'RuNet 2020' - Deploying traditional elements of combat power in cyberspace?, *Proceedings of 2017 International Conference on Military Communications and Information Systems (ICMCIS),* 15-16 May 2017, 1-8.

NIST (2017): *Robust Inter-Domain Routing*, https://www.nist.gov/programs-projects/robust-inter-domain-routing (Accessed 7 June 2017).

Nocetti, J. (2015): Contest and conquest: Russia and global internet governance, *International Affairs*, 91 (1), 111-130.

Nye, J.S. (2010): *Cyber Power*, Harvard Kennedy School: Cambridge.

Nye, J.S. (2016/2017): Deterrence and Dissuasion in Cyberspace, *International Security*, 341 (38), 44-71.

Owens, B. (2001): *Lifting the Fog of War*, The John Hopkins University Press: Baltimore.

Panarin I. & Panarina L. (2003): *Informatsionnaia voina i mir. Informatsionnoe protivoborstvo v sovremennom mire* [Information War and Peace. Information Counter Struggle in the Contemporary World], OLMA-PRESS: Mocow.

Patrushev, G.G. (2016): Servis tsentralizovannoi adaptivnoi marshrutizatsii dlia programmno-konfiguriruemikh setei [Centralized adaptive routing service for Software-Defined Networks], *12-ia Mezhdunarodnaia Aziatskaia shkola-seminar "Problemy optimizatsii slozhnykh sistem"*, Novosibirsk, 471-478.

Provy.ru (2017): *Homepage*, http://russia.provy.ru/providers (Accessed June 9th 2017).

Renesys (2013): *The New Threat: Targeted Internet Traffic Misdirection*, http://dyn.com/blog/mitm-internet-hijacking/ (Accessed 7 June 2017).

Renz, B. & Smith, H. (eds.) (2016): *Russia and Hybrid Warfare: Going Beyond the Label*, Aleksanteri Papers, 1/2016, http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf (Accessed 6 May 2017).

Reuters (2015): *In cyberattacks such as Sony strike, Obama turns to 'name and shame'*, http://www.reuters.com/article/uk-usa-cybersecurity-idUSKBN0KN2E520150114 (Accessed 3 June 2017).

RFC 882 (1983): Mockapetris, P.: *Domain names - concepts and facilities*, RFC 882. (Nov. 1983).

RFC 883 (1983): Mockapetris, P.: *Domain names - implementation and specification*, RFC 883. (Nov. 1983).

RFC 1034 (1987): Mockapetris, P.: *Domain names - concepts and facilities*, RFC 1034. (Nov. 1987).

RFC 1035 (1987): Mockapetris, P.: *Domain names - implementation and specification*, RFC 1035. (Nov. 1987).

RFC 4033 (2005): Arends R., Austein R., Larson M., Massey D. and Rose S.: *DNS Security introduction and requirements*, RFC 4033. (Mar. 2005).

RFC 4271 (2006): Rekhter, Y., Li, T. & Hares, S.: *A Border Gateway Protocol 4 (BGP-4)*, RFC 4271. (Jan. 2006).

RFC 6014 (2010): Hoffman P.: *Cryptographic algorithm identifier allocation for DNSSEC*, RFC 6014. (Nov. 2010).

RFC 6840 (2013): Weiler S. and Blacka D.: *Clarifications and implementation notes for DNS security (DNSSEC)*, RFC 6840. (Feb. 2013).

RFC 7426 (2015): Haleplidis, E., Pentikousis, K., Denazis, S., Hadi Salim, J., Meyer, D. & Koufopavlou, O.: *Software-Defined Networking (SDN): Layers and Architecture Terminology*, RFC 7426. (Jan. 2015).

RFC 8020 (2016): Bortzmeyer, S. and Huque S.: *NXDOMAIN: There really is noting underneath*, RFC 8020. (Nov. 2016)

Rid, T. (2012): Cyber war will not take place, *The Journal of Strategic Studies* 35 (1), 5-32.

Rid, T. & Buchanan B. (2015): Attributing Cyber Attacks, *Journal of Strategic Studies*, 38 (1-2), 4-37.

Rid, T. & McBurney, P. (2012): Cyber-Weapons, *The RUSI Journal*, 157 (1), 6-13.

RIPE NCC (2017): *Focus on Russia – RIPE NCC Statistics and Data*, https://labs.ripe.net/Members/fergalc/focus-on-russia-ripe-ncc-statistics-and-data (Accessed 7 June 2017).

Ristolainen, M. (2017): Should 'RuNet 2020' be Taken Seriously? Contradictory Views about Cybersecurity between Russia and the West, forthcoming in *Journal of Information Warfare,* fall 2017 issue.

Root-servers.org (2017): *Homepage*, http://www.root-servers.org/ (Accessed June 9th 2017).

Russian Federation - Official Russia (2017): *Information on RSNet Administration*, http://www.gov.ru/main/rsnet/page541.html (Accessed June 9th 2017).

RuBroad.ru (2014): *Top-10 magistral'nyk provaiderov Rossii i Top-3 krupneishikh magistral'nykh provaiderov Moskvy, 10.2.2014* [Top 10 backbone providers in Russia and Top-3 the largest backbone providers in Moscow, 10.2.2014] http://rubroad.ru/magazine/providers/4530-top- (Accessed June 9th 2017).

Sakwa, R. (2015): The Deep Rootsof the Ukraine Crisis – To Forge a Lasting Peace in Europe, We Must Rethink the Post-Cold War Security Order, *The Nation*, 4th May 2015, 300 (18), 30-32.

SANS (2016): *BGP Hijinks and Hijacks - Incident Response When Your Backbone Is Your Enemy* https://www.sans.org/reading-room/whitepapers/incident/bgp-hijinks-hijacks-incident-response-backbone-enemy-37422 (Accessed 6 May 2017).

Scott-Hayward, S., O'Callaghan, G. & Sezer, S. (2013): SDN Security: A Survey, *2013 Workshop on Software Defined Networks for Future Networks and Services*, November 11-13, 2013, 1-7.

Shlapak, David A. & Johnson, Michael W. (2016): Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of Baltics, RAND: Santa Monica.

Sheldon, J.B. (2013): The Rise of Cyberpower. *Strategy in the Contemporary World.* Baylis, J., Wirtz, J.J. Gray, C.S. (eds.) Oxford University Press: Oxford, 282-298.

Simon, H. (1977): *The New Science of Management Decision.* Englewood Cliffs, Prentice Hall: NJ.

Slayton, R. (2016/2017): What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment, *International Security*, 41 (3), 72-109.

Sloan, E.C. (2012): *Modern Military Strategy: An introduction*. Routledge: New York.

Sosenushkin, S.E. & Kruglova, P.A. (2015): Adaptivnoe upravlenie resursami informatsionnotelekommunikatsionnoi seti na osnove programmnogo konfigurirovaniia [Adaptive network traffic control based on software defined networking], *Izvestiia Samarskogo nauchnogo tsentra Rossiiskoi akademii nauk*, 6(2), 479-484.

Stone, J. (2013): Cyber War Will Take Place! *The Journal of Strategic Studies*, 36 (1), 101-108.

Strachan, H. (2013): *The Direction of War: Contemporary Strategy in Historical Perspective*, Cambridge University Press: New York.

Strategiia (2015): *Strategiia natsional'noi bezopasnosti Rossiiskoi Federatsii* [Russian National Security Strategy]," 31 December 2015, http://static.kremlin.ru/media/acts/files/0001201512310038.pdf (Accessed 1 June 2017).

Strategiia (2017): *O strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2013 gody* [The 2017-2030 Strategy for the Development of an Information Society in the Russian Federation], 9 May 2017, http://static.kremlin.ru/media/acts/files/0001201705100002.pdf (Accessed 1 June 2017).

Streltsov, A.A. & Pilyugin, P.L. (2016): K voprosu o tsifrovom suverenitete [About digital sovereignty], *Informatizatsiia i sviaz'*, 2/2016, 25-30.

Svolik, Milan W. (2012): *The Politics of Authoritarian Rule*, Cambridge University Press: New York.

Tallinn Manual (2017): *Tallinn Manual 2.0: On the International Law Applicable to Cyber Operations*. NATO CCD COE, Cambridge University Press: Cambridge.

Templeton, G. (2016): *Cyber is the new nuclear, changing the world through mutually assured disruption*, https://www.extremetech.com/extreme/233418-cyber-is-the-new-nuclear-changing-the-world-through-mutually-assured-disruption (Accessed 15 May 2017).

Thomas, T. (2001): Deciphering Asymmetry's Word Game, *Military Review*, July-August, 32-37.

Thomas, T. (2015a): Russia´s 21st century information warfare: Working to undermine and destabilize populations, *Defence Strategic Communications*, 1(1), 11-26.

Thomas, T. (2015b): *Russia – Military Strategy: Impacting 21st Century Reform and Geopolitics*, FMSO: Fort Leavenworth.

Thomas, T. (2016): *Thinking Like a Russian Officer: Basic Factors And Contemporary Thinking On The Nature of War*, January-March 2016, http://fmso.leavenworth.army.mil/documents/Thinking%20Like%20A%20Russian%20Officer_monograph_Thomas%20(final).pdf (Accessed 2 March 2017).

Trenin, D. (2016): *Should We Fear Russia?* Polity Press: Cambridge.

Tsifrovaia ekonomika (2017): *Programma:"Tsifrovaia ekonomika Rossiiskoi Federatsii" [State Project: Digital Economy of Russian Federation]*, http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (Accessed 3 June 2017).

Votel, J.L., Cleveland, C.T., Connett, C.T. & Irwin, W. (2016): Unconventional Warfare in the Gray Zone, *JFQ*, 80, 1st Quarter, 101-109.

Walt, S. (2015): Who is a Better Strategist: Obama or Putin? *Foreign Policy*, October 9th 2015. http://foreignpolicy.com/2015/10/09/who-is-a-better-strategist-obama-or-putin/ (Accessed 3 June 2017).

The Washington Post (2014): *The Sony Pictures hack, explained,* https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.80c976424e7c (Accessed 3 June 2017).

The Washington Post (2017): *More than 150 countries affected by massive cyberattack, Europol says* https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html?hpid=hp_hp-more-top-stories_hack-800a%3Ahomepage%2Fstory&utm_term=.78561b84ec9d (Accessed 3 June 2017).

Yandex.ru (2016): *Razvitie interneta v regionakh Rossii* [Regional development of the Internet in Russia], (Vesna 2016), https://yandex.ru/company/researches/2016/ya_internet_regions_2016 (Accessed 9 June 2016).

Zakonoproekt (2017): *Zakonoproekt No. 47571-7: O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii* [Bill No. 47571-7: On the Security of Critical Infrastructure of the Russian Federation], 2017 http://asozd2.duma.gov.ru/addwork/scans.nsf/ ID/EBE024490F4C5851432580810054D3AC/$File/47571-7_06122016_47571-7.PDF?OpenElement (Accessed 6 March 2017).