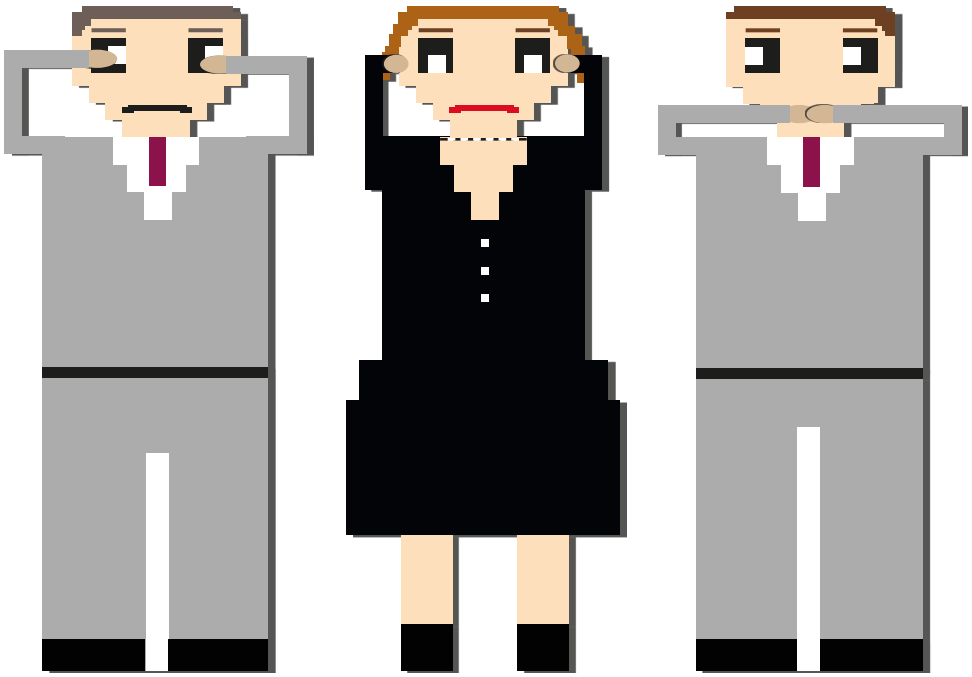
Puolustusvoimien tutkimuslaitos
Julkaisuja 11

GAME PLAYER
Facing the structural transformation of cyberspace

Edited by Juha Kukkola, Mari Ristolainen, Juha-Pekka Nikkarila



Finnish Defence Research Agency Publications 11
Puolustusvoimien tutkimuslaitoksen julkaisuja 11

GAME PLAYER

Facing the structural transformation of cyberspace

Edited by
Juha Kukkola
Mari Ristolainen
Juha-Pekka Nikkarila

FINNISH DEFENCE RESEARCH AGENCY
PUOLUSTUSVOIMIEN TUTKIMUSLAITOS

RIIHIMÄKI 2019

Cover design:
Graphic Designer
Valtteri Vanhatalo

ISBN 978-951-25-3066-3 (print)
ISBN 978-951-25-3067-0 (PDF)
ISSN 2342-3129 (printed)
ISSN 2342-3137 (online publication)

Finnish Defence Research Agency
Puolustusvoimien tutkimuslaitos

PunaMusta
Tampere 2019

Contents

Tiivistelmä

Venäjän federaatio pyrkii luomaan kyvyn kansallisen segmenttinsä irrottamiseksi globaalista Internetistä. Tavoite on kirjattu kansallisen ohjelman statuksen saaneeseen Digitaalisen talouden ohjelmaan, jonka mukaan Venäjä tavoittelee digitaalista suvereniteettia vuoteen 2024 mennessä. Toteutuessaan täysimääräisenä ohjelma tuottaisi Venäjän Internetistä aidosti kansallisen, maantieteellisesti rajatun kokonaisuuden, joka perustuisi venäläiseen teknologiaan ja kykenisi tarjoamaan kriittiset yhteydet ja palvelut ulkomaanyhteyksien katketessa. Se mahdollistaisi autoritaarisen valtion keskitetyn kontrollin informaatioyhteiskunnasta ja sen taloudesta ja tarjoaisi sotilaallisesti merkittävä edun alueellisissa tai globaaleissa konflikteissa. Ennen kaikkea se merkitsisi vapaan ja avoimen Internetin loppua ja Internetin infrastruktuuriin perustuvan kilpavarustelun alkua.

Tämä teos on jatkoa edelliselle artikkelikokoelmallemme *Game Changer: Structural Transformation of Cyberspace* (2017), joka tarkasteli sitä, miten Venäjän toimet voivat johtaa merkittävään sotilaalliseen etulyöntiasemaan kyberavaruudessa ja jopa johtaa nykyisen maailmanjärjestyksen muutokseen. Käsillä olevan teoksen artikkelit yhtäältä syventävät ymmärtämystä Venäjän politiikan historiallisista ja kulttuurisista juurista ja toisaalta tarkastelevat itse ”pelikentän” muutosta analysoimalla Venäjän hallinnon toimien vaikutusta Internetin hallintaan ja infrastruktuuriin. Artikkelit tarjoavat käsitteellisiä, teoreettisesti mallintavia ja matemaattisia ikkunoita kansallisen segmentin luonteeseen sen tosiseikan ohjaamina, että ilmiö itsessään on liian monimutkainen yhdellä näkökulmalla tai lähestymistavalla ymmärrettäväksi.

Teos ei tyydy vain kuvaamaan Venäjän politiikkaa vaan jatkaa tarjoamalla esimerkkejä siitä, miten muuttuvalla pelikentällä voitaisiin pelata. Artikkeleiden esittelemä sotapelaamisen malli on tarkoitettu kansallisten verkkojen sulkemisen vaikutusten ymmärtämiseksi – ja vastakeinojen löytämiseksi. Teoksen toiseksi viimeinen artikkeli on Ruotsin *Totalförsvarets forskningsinstitut* (FOI) tutkijoiden laatima ja tarjoaa heidän näkökulmansa aiheeseen. Edellisessä teoksessa kutsuimme kansallista ja kansainvälistä tutkijakuntaa liittymään mukaan projektiimme ja FOI:n artikkeli sekä tämän teoksen laajentunut kirjoittajaluettelo osoittavat, että kutsumme on kuultu ja siihen on vastattu.

Tässä artikkelikokoelmassa esitetyt pääväittämät ja tutkimustulokset ovat seuraavat. Venäjän pyrkimys irrottaa kansallinen segmenttinä laajemmasta Internetistä johtaa rakenteelliseen asymmetriaan ja on venäläisen strategisen kulttuurin heijastuma. Asymmetria perustuu kerroksittaiseen puolustukseen ja on matemaattisesti todistettavissa. Hanke perustuu venäläiskansalliseen ajatukseen ’yhtenäisestä informaatiotilasta’, jonka hallinta on keskitetty ja joka on vertikaalisti kontrolloitu. Kyseessä ei ole pelkkä poliittisen valtiosensuurin väline vaan pyrkimys muokata kybertaistelutilaa strategisella tasolla. Venäjä rakentaa digitaalisia rajoja luodakseen perustan ja turvatakseen digitaalisen suvereniteettinsa. Nämä rajat perustuvat maantieteeseen ja digitaalisen infrastruktuurin kansalliseen hallintaan sekä venäläiseen käsitykseen valtiosuvereniteetista. Venäjä on koonnut edellä mainitut hankkeet Digitaalisen talouden kansallisen ohjelman alle, joka täysimääräisesti toteutuessaan loisi omavaraisen, valtion valvoman ja tarvittaessa ulkomaailmasta eristettävän kansallisen informaatiotilan. Lopputuloksena on järjestelmien järjestelmä (system-of-systems), joka takaa kansallisen segmentin resilienssin konfliktijatkumon kaikissa vaiheissa aina avoimeen suursotaan asti. Tämän järjestelmän ja sen vaikutusten ymmärtämiseksi tarvitaan kaksipuolista, matrix-peli-menetelmään perustuvaa, sotapeliä niin suljettujen kuin avoimienkin verkkojen vahvuuksien ja heikkouksien analysoimiseksi. Yksi lähestymiskulma pelaamiseen perustuu kriittisen infrastruktuurin ja resilienssin arviointiin.

Huolimatta kaikesta tehdystä työstä tämä teos on vasta toinen askel pitkällä tiellä suljettujen kansallisten verkkojen aiheuttamien haasteiden ymmärtämiseksi. Paljon moninäkökulmaista ja monitieteistä työtä on vielä tehtävänä.

Introduction

Juha Kukkola
Mari Ristolainen
Juha-Pekka Nikkarila

game player
The Oxford English Dictionary defines 'game player' as "a person who plays a game or pastime; (now) specifically a person who plays a computer game or games"[1]. The Urban dictionary expands the meaning, among others, to "someone who is willing to stick with a team even when things look down"[2].

Russia has declared its aim to close off its national segment from the global Internet and to become 'digitally sovereign'. At the same time, Russia might be pursuing a decisive military advantage in cyberspace. Our previous collection of articles "Game Changer: Structural transformation of cyberspace" (2017) ended to a call to study the potential structural changes of cyberspace further. We recognized the need to comprehend this ongoing process more extensively and to find new aspects to the research. This collection of articles represents an academic response to the structural transformation of cyberspace, i.e. the 'game changer' proposed by various authoritarian states. At the moment, we propose to start playing the game by recognizing that the structural transformation of cyberspace does not threaten any specific nation. Rather, it is a threat towards the entire free and open Internet and the values it represents. To face the structural transformation of cyberspace international co-operation is required. Therefore, the concept 'game player' in the title of this collection refers to the 'open network society'[3] that needs to value openness and co-operation.

---

[1] Oxford English Dictionary 2018 s.v. 'game player', [Online] https://en.oxforddictionaries.com/definition/game-player, [Accessed 29 October 2018].
[2] Urban dictionary 2018 s.v. 'game player', [Online] https://www.urbandictionary.com/define.php?term=game%20player, [Accessed 29 October 2018].
[3] An open network (i.e. global Internet) is defined in our studies 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, equal access to knowledge etc. Open network nations share the values of open networks and their segment of the Internet is built on those principles. The open network society is a collection of the above defined nations. A contradictionary concept used is 'a closed network nation' that

A ‘game player’ invents and intensively develops new solutions collectively that is the only way to answer the political and military challenge of closed networks.

During the writing process of this collection we have become acutely aware that the study of closed networks and ‘digital sovereignty’ is inherently a multidisciplinary problem. Its effects are manifold and it can be approached as a political, military, economic, legal, technological or even a cultural issue. It is an issue that requires a wide range of expertise to be addressed properly. This is why we have invited the Swedish Defence Research Agency to collaborate with us and to provide their perspective on the problem at hand.

The articles in this collection have been organized under four sections: 1) State of the game, 2) Understanding the ‘game board’, 3) Playing the game and 4) Joining forces. All the research articles (except one) are internationally peer-reviewed conference papers that have been presented and published in different conference proceedings in 2018. One article is a research bulletin published by the Finnish Defence Research Agency. Referencing is done according to the guidance of the original publication. The original sources are indicated on the first page of the article in question. The invited concluding remarks in the final section propose questions for joint research in the future.

The authors of the research articles represent the Finnish National Defence University and Finnish Defence Research Agency. Invited authors represent the Swedish Defence Research Agency. Detailed author information follows this introduction.

1 State of the Game

The first section contains an article that provides background information and explains the state of the game. The Russian Federation aims to be an independent cyber superpower. Russian national cyber power is partly based on structural changes of the Internet governance. The first article of this collection “Russian cyber power and structural asymmetry” argues that by developing so-called ‘digital sovereignty’ the Russian Federation is intentionally creating an asymmetric advantage in cyberspace. This

is understood 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 technically separated from the global Internet.

‘structural cyber asymmetry’ is both a defensive and offensive resource of national cyber power. By shaping and delineating cyberspace on technical, syntactic, and semantic levels with technical, administrative, and political tools to a closed national network, Russia achieves a disproportionate military advantage on the strategic level.

2 Understanding the Game Board

Articles in the second section aim to understand the ‘game board’. In cyberspace, as on any ‘game board’, it is necessary to understand the surface marked to play the game, and on which the counters or other pieces are placed or moved.

The second article of this collection “Civilian and military information infrastructure and the control of the Russian segment of the Internet” explains how the Russian Federation is constructing the basis for national control of the Internet. This article provides an overview of the principles and practices of this project and, moreover, examines how Russia implements the concept of ‘the unified information space’ in building the ‘national segment of the Internet’. The main aim of this article is to find answers to the question how Russia is preparing to protect and control its national networks. Specifically, it seeks answers to the question of how ‘the unified information space’ is structured in civilian and military spheres based on the categories of infrastructure, services, and authorities responsible for creating, monitoring, and controlling this space. This article argues, firstly, that the distinct Russian idea of ‘unified information space’ affects the way it strives to shape cyberspace. Secondly, the article argues that although the national segment of the Internet in Russia has been developed by private actors, it is increasingly subjected to centralized civilian and military control. Thirdly, this process is not just about censorship or the control of information, but has a definite military strategic character built into it.

The third article “Projected territoriality: A case study of the infrastructure of Russian ‘digital borders’” continues to investigate the infrastructure of the Russian segment of the Internet by broadening the view to ‘digital border’ formation processes. This article is a case study of the delineation, protection and control processes of the Russian ‘digital borders’. Moreover, it represents an original attempt to demonstrate how territoriality can be projected into cyberspace on the level of infrastructure of an individual country. In order to ensure Russian ‘digital sovereignty’ the ‘digital borders’ of a national segment of the Internet need to be firstly delineated,

secondly protected, and thirdly, cross-border control needs to be organized. This article describes how 'digital borders' are constructed through a vertical and horizontal combination of authorities and infrastructure within the Russian national segment of the Internet. These 'digital borders' could ensure undisturbed functioning of this national segment which could be considered as a certain model for future 'digital border security', i.e. a form of cyber security.

The forth article "New guidance for preparing Russian 'digital sovereignty' released" explains how the Program of the Digital economy of the Russian Federation (*Tsifrovaia ekonomika Rossiiskoi Federatsii*) is being planned to be implemented in the light of the action plans approved in January – February 2018. This article focuses on 'directions' (*napravlenie*) of 'information security' (*informatsionnaia bezopasnost'*) and 'information infrastructure' (*informatsionnaia infrastruktura*) of the 'Digital economy'. Furthermore, 'directions' are approached through the concepts of shaping of cyberspace, controlling the national segment of the Internet, and 'digital sovereignty'. These concepts connect the 'Digital economy' and its 'directions' to the project started by the Russian government in 2014 to create a self-sustained national Internet. This article stresses that Russian 'digital' socio-economic plans have also a military strategic character.

The fifth article starts modelling the game board. The "Modelling closed national networks – Effects in cyber operation capabilities" article introduces a mathematical model to describe how operational capabilities are affected when a nation closes its national network. The aim of the article is to model the defensive capability of a closed national network to protect the critical infrastructure of a closed network nation. A mathematical expression for the capability is resolved. Furthermore, the solution is utilized to evaluate the defence of an exemplary critical infrastructure. It is demonstrated that the defensive capability of a closed national network in protecting the exemplary critical infrastructure is significant. It is acknowledged that a more sophisticated model is required in order to describe the effects of a closed national network in more detail. Nevertheless, the model proposed in this article extends the analysis of how a closed national network affects the operational capabilities at the overall system level. The model may be used to form and improve situation awareness as the process evolves.

The sixth article "The Russian segment of the Internet as a resilient battlefield" continues the description of the game board by claiming that Russia is building a system-of-systems of cyber security and defence measures that it believes enables it to withstand cyber-attacks against its

critical national assets. The subsystems of this entity have different functions and are controlled by various actors, but can be joined to a centrally controlled system. This article builds on previous research into Russian cyber strategy by aiming, firstly, to describe the developing national system-of-systems and, secondly, to analyse its effects on the resilience of the national segment of the Internet during peace time, intensified competition, conflict and war. The paper argues that the Russian Federation is aiming for a flexible, although complex and possibly vulnerable, national cyber defence system that could ultimately provide it with a decisive advantage in a state-to-state cyber conflict.

3 Playing the Game

Articles in the third section start 'playing the game' and explore the possibilities of wargaming when investigating the structural changes of cyberspace. The seventh article "Wargaming a closed national network: What are you willing to sacrifice?" points out that the closing of a national network could cause a situation where the rest of the 'open network society' is forced or wish to consider closing their national networks as well. A situation where national governments substantially restrict information flows and connectivity of the network could cause serious effects to the critical infrastructure, economy, and alliances. This article proposes a wargaming framework to analyse the effects of closing the national network on hostile actors operating critical infrastructure and who rely on the openness of that network for their operations. This article provides information on what nations planning to close their network need to take into consideration, while offering a strategic insight for those actors who are confronted by a nation closing its network.

The eight article, "Wargaming the cyber resilience of structurally and technologically different networks" reviews different analytical frameworks and suggests that a table top cyber wargame is to be applied when trying to analyse the effects that closed national networks could impose in the near future. The scope of the wargame is to extract results of how the resilience of an open national network differs from a closed national network. It is self-evident that the formation process of resilience is different between the diverse systems. The proposed wargame is a two-sided cyber table top wargame. The wargame is based on at least two blue teams, at least one red team and a control team (namely a white team). One blue team is located in the closed national network and its system relies on closed national network infrastructure. The other blue team operates its system within an open network society. By designing, constructing and

executing the proposed cyber wargame we argue it is possible to find these differences and similarities as well. Current research improves cyber situation awareness and proposes a direction to follow when trying to understand the changing circumstances of cyber space. It also suggests how research resources could be directed when trying to improve the situation awareness of the closing process.

4 Joining Forces

In the fourth section we have given free word to the researchers of the Swedish Defence Research Agency (FOI). The epilogue presents their assessments and gives suggestions for future research topics. The researchers of FOI remind us of the need to continuously and critically evaluate the Russian project to control its national segment of Internet. The drive towards 'digital sovereignty' and asymmetry might have unseen problems and consequences and, additionally, cyberspace and the technologies it is based upon are continuously evolving. To understand all these interrelated and developing issues future research is required.

Authors

Simo Huopio is currently working as a Senior Research Scientist, Cyber Defence, at the Finnish Defence Research Agency (FDRA). He got his Masters (CS) from the Helsinki University of Technology in 1999 and has since worked in multiple mobile and information security roles in F-Secure and Nokia before joining the Finnish Defence Forces. In additional to his researcher position he is a doctoral student at the University of Oulu. His professional interests include software robustness testing, threat analysis and practical cyber defence capability development.

Juhani Hämäläinen PhD (theoretical physics) is a Chief Scientist at the Finnish Defence Research Agency. He has been conducting research in the military context since 2000. His research interests covers mathematical modelling and methodology development for different research applications.

Margarita Jaitner received her MSSc in Societal Risk Management in 2013 at Karlstad University Sweden. Her research focuses on the area of information warfare in cyberspace—with a particular focus on Russian operations, as well as hybrid warfare and policy-related research within cyber security. She has previously conducted research at the Swedish Defence University, Blavatnik Interdisciplinary Cyber Research Center in Tel Aviv as well as the Finnish Defence University. She currently works as an analyst at the Swedish Defence Research Agency (FOI) as well as at the Swedish Defence Forces.

Vesa Kuikka obtained the degree of licentiate in Philosophy in physics in 1986 from the University of Helsinki and in mathematics in 2004 from Åbo Akademi. Vesa Kuikka is a Fellow of the Actuarial Society of Finland (FASF). He works at the Finnish Defence Research Agency as a member of the mathematical modeling team. His research interests are in modelling complex networks, military capabilities and macroscopic level combats.

Captain (army) **Juha Kukkola** has a Master's degree in Political science (2005) and Military science (2008) and works as a Research Officer at the Finnish National Defense University (FNDU). He is currently writing his doctoral thesis on Russia's military cyber power and strategy. He has served in the Finnish Defense Forces from 2008 as a platoon leader, signals officer, staff officer and lecturer and has specialized in air defense, C4 systems and Russian and Cyber studies.

Major **Heikki Lantto** works as a Senior Research Staff Officer at the Finnish National Defence University (FNDU) and is a doctoral candidate in military sciences at the FNDU. His main research area is wargaming in operational warfare. A career officer from 2001 and has had various posts in signals, communications, R&D and lecturing positions during his service in the Finnish Defense Forces. He has specialized in C4 systems, wargaming and operational warfare.

Captain (Eng.), Dr. **Juha-Pekka Nikkarila** has a PhD in Physics (2008) and serves as a Researcher and a Special Officer at the Finnish Defence Research Agency (FDRA). He obtained his MSc in Physics (2006) and MSc(Tech.) in Electrical Engineering (2016). He has served at FDRA since 2012 with research interests in operation analysis, electronic warfare and Cyber studies. His current research interests include modelling Cyber influencing, resilience and warfare. Earlier he served as a researcher in Marioff Corporation / United Technologies Corporation (2009-2012), Inspecta (2007-2009) and at the University of Jyväskylä (2006-2007), as well as a physics lecturer in Metropolia University of Applied Sciences (2009-2014).

Dr. **Mari Ristolainen** is a Researcher at the Finnish Defence Research Agency. She has studied psychology at the Moscow State University and she earned a doctorate in Russian Language and Cultural Studies from the University of Joensuu in 2008. She has been conducting postdoctoral research in the field of Russian and Border Studies in several Academy of Finland- and EU-funded projects at the University of Eastern Finland and at the University of Tromso, Norway. Her current research interests include cyber warfare as a phenomenon, Russian digital sovereignty, and the governance of cyber/information space.

Teodor Sommestad received his PhD degree in 2012 Industrial Information and Control Systems and his MSc degree in Computer Science in 2005, both at the Royal Institute of Technology (KTH) in Stockholm, Sweden. His previous research covers topics such as security assessments, network intrusion detection, and information security culture. He is currently deputy research director at the Swedish Defence Research Agency (FOI) where he manages the organization's research program on operations in the cyber domain.

Marko Suojanen is a Principal Scientist at the Finnish Defence Research Agency. He holds an M.Sc. in electronics from Tampere University of Technology. Mr. Suojanen has worked in research and R&D projects in several areas at Tampere University of Technology, the Technical Research

Centre of Finland and technology companies before his career in defence. His research interests include wireless communications, technology foresight, systems engineering and operational analysis. He has been active in international co-operation efforts and conferences. Mr. Suojanen is the author of the book Military Communications in the Future Battlefield that was published by Artech House in 2018.

Commander (GS) **Topi Tuukkanen** currently serves as Cyber Research Manager with the Finnish Defence Research Agency. He graduated from the Naval Academy in 1988 and started his service as a weapons officer on a number of surface combatants. He entered the domain of Command, Control and Communications after having received a B.Eng. degree in computer sciences in 1992. After a general staff course in 1997 he served as the M6 (CIO) with the Finnish Navy HQ in which position he faced the Y2K event. Furthermore, he has participated in the establishment of SUCFIS sea surveillance cooperation between Finland and Sweden and in the establishment of the European Software radio program ESSOR. Since then he has served as the C3 representative to NATO and the EU in Brussels. Besides his current duties, he is pursuing a PhD in wireless communications with the University of Oulu.

Lieutenant Commander (Eng.), Dr. **Bernt Åkesson** has a Master's degree in Chemical Engineering (2000) and a Doctoral degree in Process Control (2006). He has served in the Finnish Defence Forces since 2007 and currently works as a Division Engineer at the Finnish Defence Research Agency. His current research interests include modelling and simulation of cyber operations.

STATE OF THE GAME

Russian Cyber Power and Structural Asymmetry

Juha Kukkola

Abstract

The Russian Federation aims to be an independent cyber superpower. Russian national cyber power is based on structural changes of the Internet governance. This paper argues that by developing so-called 'digital sovereignty' the Russian Federation is intentionally creating asymmetric advantage in cyberspace. This 'structural cyber asymmetry' is both a defensive and offensive resource of national cyber power. By shaping and delineating cyberspace on technical, syntactic, and semantic levels with technical, administrative, and political tools to a closed national network, i.e. RuNet, Russia achieves a disproportionate military advantage on the strategic level. Firstly, this paper presents the concept of 'structural cyber asymmetry' to challenge traditional notions of asymmetry and cyber power. Secondly, it examines influential Russian military academic writings and most important policy documents to understand how Russians perceive cyber power and the shaping of cyberspace on the strategic level. Thirdly, it provides a discussion on the effects of 'structural cyber asymmetry' on Russia's national cyber power. This paper shows that although there are significant terminological and conceptual differences between Western and Russian understandings of cyber issues, 'structural cyber asymmetry' provides a beneficial tool for understanding Russian cyber policy. It resonates decidedly better with Russian strategic cultural thinking than traditional Western concepts. This paper also provides a fresh theoretical view on Russia's cyber policies and finds evidence that Russia is intentionally shaping cyberspace to enhance its military cyber power. The overall aim of this paper is to increase understanding of Russian security and military strategy in cyberspace by using novel concepts and original, Russian language sources.

Keywords: Russian cyber power, Structural asymmetry, Digital sovereignty, RuNet, Closed national network

The first version of this paper was published and presented at the 13th International Conference on Cyber Warfare and Security (ICCWS), 8-9 March 2018, Washington DC, USA.

1 Introduction

The future of the Internet as a borderless, open, free and secure sphere of human activity is challenged. It is confronted by the will of some nation states to apply the principles of territorial sovereignty to the Internet. This process has been called the birth of 'Cyber Westphalia', and it will affect how we conceptualize and utilize cyber power now and in the future (Demchak & Dombrowski, 2011; Demchak & Dombrowski, 2013). Starting, at the latest, from 2014 the Russian Federation has been at the forefront of this process (Sovet Bezopasnosti Rossiiskoi Federatsii 2014). It codified this process in policy by releasing its new Information Security Doctrine in 2016 (Doktrina, 2016) which was aimed at controlling the Russian segment of the Internet, summarized as 'digital sovereignty' (Tsifrovaia ekonomika, 2017; Strategiia, 2017; Yefremov, 2017). Mari Ristolainen has argued that this project 'RuNet 2020' is aimed at a safe, closed, and fully state controlled Internet and that we should take this project seriously (Ristolainen, 2017). The declaratory aims of 'RuNet 2020' are related to national security especially in the information sphere. As has been argued in further studies, the building of a closed national network is not only a defensive measure. It might also have an offensive aspect, and have a profound impact on military cyber power balance to the disadvantage of states relying on safe, open and secure Internet principles. This phenomonen has been identified as 'cyber asymmetry' (cf. Kukkola et al., 2017).

Recent studies on Russia's military and security policies have shown that the Russian approach to deterrence is more comprehensive than Western ones and that a search for asymmetry is part of it (Thomas, 2015; Bruusgaard, 2016; Adamsky, 2017). Built on this view of deterrence, centrally state controlled mobilization of material and human resources is still a valid policy in Russian security politics (Cooper, 2016). If we combine these observations with the perceived blurring of the distinction between peace and war (Wirtz, 2017), the study of Russian cyber power on a strategic level is a highly topical research agenda.

In this paper, I further develop the idea of 'cyber asymmetry' and define it more rigorously as 'structural cyber asymmetry.' I also argue that some states strive to achieve 'structural cyber asymmetry' based on their historical, culturally bound, strategic thinking. Overall, the aim of this paper is to increase understanding of Russian security and military strategy in cyberspace by using novel concepts and original, Russian language sources. The first part of this paper is an introduction. The second part is a

conceptual analysis of 'structural cyber asymmetry.' It is based on previous studies of cyberspace, cyber power, military strategy and military asymmetry. The third and fourth parts are qualitative content analyses of leading Russian military journals from the period of 2000-2017. I show how Russians understand military asymmetry, how they discuss the shaping of cyber space, and how asymmetry is understood in these discussions. The fifth part goes on to analyse the principal doctrines and strategies of the Russian Federation. In it, I show that the documents reflect the ideas presented in journals and that doctrines and strategies could lead to 'structural cyber asymmetry.' In the sixth part, I provide a synthesis and discussion on asymmetry and Russian cyber power.

2 Structural Cyber Asymmetry

The concept of 'structural cyber asymmetry' is based on the premise that cyber power is a contextual and relational phenomenon. It only gains meaning through the situation it is used in (Baldwin, 1989; Guzzini, 1993). In this paper, power is understood to be used in and through cyber space which is understood as "an electronic medium through which information is created, transmitted, received, stored, processed and deleted" (Godwin III, et al., 2014). Cyber space is a man-made and malleable environment, and a domain of human activity that has its own characteristics which affect the use of power (Libicki, 2007). From these premises, I derive the following definition of cyber power: "an ability that empowers an actor to influence others in or through cyber space and to shape it to its advantage according to its preferences" (Cf. Endresen, 2016). The use of cyber power is intentional, although not always strictly rational, and, as such, is tied to the ideas and beliefs actors have concerning power, its use, and the world at large (Gray, 1999). This is reflected in the kind of strategies actors choose to utilize power. It should be emphasized that these cyber strategies, understood as planning, preparation and action, are always implemented against an opponent that has power and will of its own (Luttwak, 2001).

In Western military thinking, asymmetry has been connected to 'asymmetric warfare' or 'conflict' since the 1970s (Freedman, 2013). Basically, asymmetric warfare came to be defined as warfare by non-state actors against a military superpower or coalition that relied on high-tech conventional capabilities and methods and was restrained by fear of casualties and collateral damage (Evans, 2005). An approach to asymmetry based on means and methods is, however, too narrow. The reason is, firstly, that there is more to asymmetry than non-state actors and unconventional means. Secondly, cyberspace is artificial and can be shaped according to

the security needs of states. Thirdly, some states are willing to depart from the idea of global commons towards nationally controlled closed networks. And fourthly, closed networks provide both defensive and offensive advantage (Kukkola, et al., 2017, 166). It has even been proposed that asymmetry is part of every conflict and 'asymmetric warfare' is a-historical misnomer (Strachan, 2013). Building on previous studies (cf. Kukkola, et al., 2017), I propose 'Structural cyber asymmetry' as a different kind of approach. It is based on the notion that the shaping of cyberspace by creating a closed national network creates asymmetry in power. It is a disproportionate, exploitable imbalance between actors (Oehmen & Multari, 2014). Cyberspace can be analyzed as 'digital territory' consisting of distance between points (hops), borders between subspaces (Firewalls, filtering, routing, subnetworks and AAA –policies etc.) or environment (electromagnetic radiation, protocols, information processes). The nature of this territory affects actors.

'Structural cyber asymmetry' is a relational and structural concept. Although structural asymmetry is connected to the resources of a nation, asymmetry is not a direct result of utilizing those resources, but is intermediated by the attributes of cyberspace. Structural asymmetry is not, then, a resource or capacity of actor, but an attribute of cyberspace. Digital territory is not shaped directly. Cyberspace is affected by technology, governance, politics and norms. By studying these, it is possible to see where, when and how asymmetry is deliberately or unintentionally created. Asymmetry provides advantages through differences in the quality of situation awareness, speed of decision-making, and freedom of action. By comparing these three elements between belligerents, it is possible to make observations on disproportioned advantages. The effects of 'structural cyber asymmetry' on the strategic level relate to ways to use force. It is argued that asymmetry through the closing of national networks provides a belligerent a definite advantage in deterrence, in controlling the way conflict evolves, and in threatening an opponent from a position of strength. (Kukkola, et al., 2017, 171).

3 Russian Asymmetry as a Strategic Response

The concept of asymmetry is most often used in Russian journals in the context of 'asymmetric response' (*asimmetrichnii otvet*). Asymmetric response can be considered as a 'genuine' Russian concept and it gives the context to Russian understanding of asymmetry. 'Asymmetric response' was first used during the 1980s, when the Soviet Union tried to counter the United States' Strategic Defense Initiative and AirLand Battle doctrine.

Later, it has become a catch phrase meaning cost-effective solution to military unbalance between great powers (Kokoshin, 2007).

'Asymmetric response' is defined by other concepts. First is the rather consistently defined concept of military power (Kirillov, 2005). Military potential (*potentsial*) consists of all material and moral resources that can be mobilized as military power (*moshch'*) through states' military policy. Strategy utilizes military power by planning, organizing and conducting the use of force through forces and means (*sily i sredstva*) and forms and methods (*formi i sposoby*). The perceived change in the character of war in the 2000s – 2010s has highlighted the role of peace time, non-military, indirect, and asymmetric action as part of military strategy (Kartapalov, 2015; Gerasimov, 2017). The second defining concept is that the Russian Federation is a great power (*derzhava*), so asymmetry for Russia is related to the balance of power between great powers (Strategiia, 2015). The third defining concept is 'counter struggle' (*protivoborstvo*). It derives from Russian strategic culture which is based on the Soviet past and the Cold war. Basically, it presupposes that relations between great powers are constant dialectical struggle for pre-eminence with all means at their disposal (Babich, 2008; Shalamberidze, 2011). The fourth one is strategic deterrence (*strategicheskoe sderzhivanie*). Strategic deterrence is a complex set of measures to anticipate threats, persuade, threat, and coerce aggressors, and if needed, to restrict escalation and inflict unbearable costs on aggressors. It has a peace time function to protect interests, neutralize threats and a war time function to eliminate them. (Khriapin & Afanas'ev, 2005; Matvichuk & Khriapin, 2010). The above mentioned concepts should be understood as parts of Russian strategic culture which is state-centric and antagonistic to the United States and NATO (Strategiia, 2009; Strategiia, 2015).

'Asymmetric response' has been a recurring theme in Russian military discussions during 2000-2017 (Mikhailov, 1999; Kolyvanov, 2006; Gorbachev, 2006; Kulakov, 2008; Chekinov & Bogdanov, 2012; Kartapalov, 2015; Gerasimov, 2017). It can be summarized as a military strategic idea that promises a cost-effective solution for strategic deterrence against perceived threat. Aspiration to military parity or symmetry with all costs is anathema because it is perceived to have led to the collapse of the Soviet Union. Instead, vaguely defined indirect and asymmetric actions or means should be developed and used. They are based on protecting national critical assets, finding out potential opponent's weaknesses, developing ways to threaten those weaknesses (creative use of resources at hand or developing innovative technology), forecasting the future, obfuscating an opponent about real capabilities, and neutralizing possible threats through

military means, diplomacy, politics, economy and information 'counter struggle'. Advantage should be sought already in peace time. 'Asymmetric response' has been used to define actions against the United States' missile defence program and cyber capabilities, Prompt Global Strike program, Network Centric Warfare (NCW) concept, use of 'colour revolutions' and lately against 'controlled chaos' or the United States' and NATO's 'hybrid war' against Russia.

The concepts of 'structural cyber asymmetry' and 'asymmetric response' resonate quite well with each other. There are the same elements in both and the creation of a closed national network could be considered as protecting critical assets (information and infrastructure) to gain asymmetric advantage cost-efficiently, and as providing added means of deterrence in addition to conventional military and nuclear ones.

4 From Weakness to Strength – Information Asymmetry

Russian military journals were already discussing 'information warfare' (*bor'ba*) in the beginning of the 2000s (Kalinovskii, 2001). Some claimed that in the context of 'informatization' (*informatizatsiia*), information confrontation takes primacy over armed warfare. Its essence was the battle for information supremacy (*prevoskhodstvo*) which alone could achieve political objectives (Bogdanov 2003). Others contested this view, and sought more restricted, operationally useful definition (Gorbachev, 2006; Orlianskii, 2002 & 2008). The militarization of information space worried Russians already in 1998 when they put forward in the United Nations their proposal on international information security. In their view, the United States dominated the Internet and used it to threaten less developed states with 'information weapons'. (Dylevskii, et al., 2007). On the operational-tactical levels Russians were trying to solve, how NCW could be applied to their armed forces and how new means of information warfare (with competing definitions) should be integrated into the current doctrine (Vypasniak, 2009; Dul'nev, et al., 2011). On the strategic level, Russians developed the concept of Unified military information space. It was based on the United States' Defense Information Systems Network (DISN) (Sherstiuk, 2003; Karpov, et al., 2004).

'Informatization' has been presented both as a military threat and as a possibility. It was a threat because Russia was lagging behind its potential opponent in the information sphere and that opponent controlled the Internet (Molchanov, 2008; Litovkin, 2011). The Internet, as defining part

of information space, is perceived as a national security interest for Russia. Possibilities, which were thought as asymmetric responses, were: international control over 'information weapons' (Dylevskii, et al., 2007), cheapness of information-technological means (compared to e.g. nuclear weapons) (Kalinovskii, 2001), counter-C2 against NCW by using Electronic Warfare (Dul'nev, et al., 2011), and, most interestingly, creation of unified military command and control system (EASU). The last one is based on an idea developed in Soviet times, and is based on a national, inter-governmental, hierarchical, command and control network. (Baraniuk, 2003; Korytko & Sheptura, 2011). It is an example of how strategic culture shapes the thinking about information warfare in Russia.

In the beginning of the 2010s military journals published articles on conceptual differences of cyber space and information space. They referred to Western, mainly American, academic studies and policies, and to domestic academic studies. One of the main conceptual problems was, how to separate or combine cyber, electronic and information (psychological) warfare (Antonovich, 2011; NVO, 2013). A kind of compromise was information-technological warfare which defined means as technological but objects as ranging from infrastructure to decision-making and the will of the opponent (Strel'tsov, 2011; Chekinov & Bogdanov, 2012). Cyber, as a term, almost never appeared in official documents (cf. Doktrina, 2016). Discussions in the journals were probably affected by the official use of the term 'information' instead of 'cyber', although cyber was still used up to 2017 in some articles (Gerasimov, 2017).

Around 2011 the new threat of 'controlled chaos' and later 'hybrid war' strengthened demands for, on the one hand, controlling the national information space, and, on the other hand, ensuring access to the global information space in case of a blockade. (Kuznetsova, 2013; Vorob'ev & Kiselev, 2014). The 'information counter struggle' was also elevated to the realm of national and military security, and strategic deterrence was given an information component (Gryzlov & Pertsev, 2015; Chekinov, et al., 2015; Romashkina & Koldobskii, 2015). Information (in its technological and psychological dimensions) was now considered to have a strategic effect which required a militarized, whole-of-government approach (Dylevskii, et al., 2016). Clearly disillusioned by Russia's unsuccessful bid to create an international agreement to ban 'information weapons', Russian writers proposed more regional arrangements for information security (Beliantsev, et al., 2015; Dylevskii, et al., 2016).

None of the articles studied in this paper directly refers to cyber or information-technological 'power' or 'digital sovereignty.' Although, it

should be noted, that the term 'information power' (*informatsionnaia moshch'*) has been described in other sources as information infrastructure, scientific- technological potential, intellectual potential, means of information counter-struggle etc. (cf. Beprintev, 2011). In the articles, power is implicitly present as aspects of military security and power: as information, technological, and economic potential. Its negation, weakness, is associated with vulnerabilities of critical information infrastructure, deficiencies in military automatic command and control systems, dependence on foreign technology and level of education. 'Digital sovereignty' is also implicitly present, as many authors state that states will fall prey to stronger ones if they do not control their information space and devolop their capabilities (Chekinov & Bogdanov, 2015; Chekinov, et al., 2015).

The United Sates was presented as a potential opponent in the 2000s and later as a clear and present enemy in the information sphere. Russians acknowledged that they were weaker than the United States technologically and economically, and a response (*otvet*) was needed. The search for asymmetry is implicitly, and in some texts explicitly, present. Russia must contain the United States and NATO with international agreements and with cooperation with willing partners, and it must develop technical means which are based on vulnerabilities of more developed states, and protect itself from the use of information-technical use of force. This is partly done by shaping cyberspace.

5 Asymmetric Ideas into Action

The Russian Federation's National security strategy (Strategiia, 2015) states that information security is part of national security, and that national security is ensured by information (partly technological) means. Information means are part of strategic deterrence and the prevention of military threats. Critical information infrastructure is one of the objects of information threats. According to the Military doctrine of Russian Federation (Doktrina, 2014), military threats are present in information space (*informatsionnoe prostranstvo*). These emanate from the use of 'information or communication technology' against, inter alia, sovereignty and territorial integrity. To reduce these threats all security organizations should be connected to a unified network. Also, one of the tasks of the armed forces is the construction of an information management system and its integration with automatized command and control systems on all levels of military hierarchy. Military policy of the Russian Federation includes cooperation on information-technological issues with interested states.

The Russian Federation's doctrine of information security (Doktrina, 2016) states that Russia has national interests in the information sphere (*informatsionnaia sfera*). Protection of critical information infrastructure, which may reside outside Russia's borders, and of a unified communications network, in peace time, under threat, or during war, is one of Russia's national interests. One other interest is protection of sovereignty in the information sphere. These interests are threatened by foreign counties using information-technological means. In the context of military defence, Russia responds to these threats with strategic deterrence and by ensuring protection of its systems with, inter alia, information forces and means. Russia also enhances the stability (*ustoichivost'*) of its critical information infrastructure and avoids giving control of its infrastructure to foreign actors. Lastly, in the context of strategic stability, Russia ensures information security by "developing national management system of the Russian part of the Internet." This should be done in a centralized and vertical fashion.

The strategy of the development of the information society in the Russian Federation 2017 – 2030 (Strategiia, 2017) is based on the documents mentioned above. The strategy states that to protect the critical information infrastructure of the state and national telecommunication networks, regulation, centralized monitoring and control of information systems and networks must be ensured. These objectives are achieved, for instance, by independent functioning of the Russian segment of the Internet which requires state control of this segment. Based on the strategy, the Russian government updated its State program 'Digital economy of the Russian Federation' (Tsifrovaia ekonomika, 2017) which states that in information security Russia shall achieve 'digital sovereignty' in 2020. All the documents addressed here highlight the importance of developing and protecting the scientific-technological and economic base of the state.

The drive to unify and control national cyber space is clearly present. So is the desire to respond to the perceived threats from information space. The main elements of this response are the ability to close out threats, the establishment of organizations to deter threats, the reduction of threats by regional cooperation, and the development of a strong digital economy. It should be noted that none of the documents mention asymmetry or aggressive intentions, only prevention and deterrence.

6 In conclusion

Based on the analysis presented in this paper Russians have not been so much interested in elements of cyber power but instead in its implementation. Their discussions in academic journals and policy documents are threat-based, defensive. Still, Russians have a well-defined concept of military power which includes information-technological potential. Also, as they are routinely discussing the United States' cyber capabilities, they are implicitly discussing about their own strengths and weaknesses. They recognize the asymmetry in this relationship and try to find responses to it, asymmetrically. Their answer is, firstly, to protect themselves by applying the principles of territorial sovereignty to cyber space. The 'nationally controlled part of the Internet' enables them to threaten potential aggressors with less fear of surprise attack or retaliation. Secondly, they try to find cost-effective solutions to maintain their strategic deterrence. This is done by finding out technological weaknesses and investing on cost-effective technological innovations. Thirdly, through diplomacy and alliances Russians acquire ways to go around 'digital blockades' or 'sanctions.' International norm building is part of the strategy. Based on journals and official documents studied in this paper, it is possible to argue, that elements of building 'structural cyber asymmetry' are present in Russian military security thinking and policies. Whether this is intentional policy or not, is an open question. However, the shaping of cyber space in the spirit of 'cyber Westphalia' is progressing and its implications for global military security should not be taken lightly.

References

Adamsky, D., (2017) From Moscow with coercion: Russian deterrence theory and strategic culture. *Journal of Strategic Studies*. [Online] Available at: *https://doi.org/10.1080/01402390.2017.1347872* [Accessed 5 August 2017]

Antonovich, P. I. (2011) O sovremennom ponimanii termina «kibervoina». *Vestnik Akademii voennykh nauk,* 35(2), pp 89-96.

Babich, V. V. (2008) O novom podkhode k analizu sovremennogo protivoborstva i nekotorykh drugikh problemakh. *Voennaia mysl'*, 2008(3), pp 33-42.

Baldwin, D. A. (1989) *Paradoxes of Power.* New York: Basil Blackwell.

Baraniuk, V. V. (2003) Edinoe informatsionnoe prostranstvo VS RF: problemy sozdaniia. *Voennaia mysl',* 2003(3), pp 36-38.

Beliantsev, A. E., Lymar, A. V. & Kazachenko, A. N. (2015) Informatsionnaia bezopasnost' kak vazhneishii faktor gosudarstvennoi informatsionnoi politiki Rossiiskoi Federatsii. *Vestnik Akademii voennykh nauk,* 52(3), pp 79-84.

Bogdanov, S. A. (2003) Veroiatnyi oblik vooryzhennoi bor'by budushchevo. Voennaia mysl', 2003(12), pp 2-7.

Bruusgaard, K. (2016) Russian strategic deterrence. *Survival,* 58(4), pp 7-26.

Chekinov, S. G. & Bogdanov, S. A. (2012) Strategicheskoe sderzhivanie i natsional'naia bezopasnost' Rossii na sovremennom etape. *Voennaia mysl',* 2012(3), pp 11-20.

Chekinov, S. G. & Bogdanov, S. A. (2015) Voennoe iskusstvo na nachal'nom etape XXI stoletiia: problemy i suzhdeniia. *Voennaia mysl'*, 2015(1), pp 32-43.

Chekinov, S. G., Bogdanov, S. A. & Popov , O. B. (2015) Problema sovremennoi voennoi bezopasnosti Rossii v usloviakh globalizatsii. *Vestnik Akademii voennykh nauk,* 53(4), pp 172-181.

Cooper, J. (2016) *What If War Comes Tomorrow: Who Russia Prepares for Possible Armed Aggression.* Whitehall Report 4-16*,* London: RUSI.

Demchak, C. & Dombrowski, P. (2011) Rise of a Cybered Westphalian Age. *Strategic Studies Quarterly,* Spring, 5(1), pp 32 - 61.

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

Doktrina (2014). *Voennaia doktrina Rossiiskoi Federatsii.* [Online] http://www.scrf.gov.ru/security/military/document129/ [Accessed 4 October 2017].

Doktrina (2016) *Dokrina informatsionnoi bezopasnosti Rossiiskoi Federatsii.* [Online] http://static.kremlin.ru/media/acts/files/0001201612060002.pdf [Accessed 2017 September 22].

Dul'nev, P. A., Kovalev, V. T. & Il'in , L. N. (2011) Asimmetrichnoe protivodeistvie v setetsentricheskoi voine. *Voennaia mysl',* 2011(10), pp 3-8.

Dylevskii, I. N., Komov, S. A., Korotkoe, SV., Rodinov, S. N. & Fedorov, A. V. (2007) Voennaia politika Rossiiskoi Federatsii v oblasti mezhdunarodnoi informatsionnoi bezopasnosti: regional'nyi aspekt. *Voennaia mysl',* 2007(2), pp 32-40.

Dylevskii, I. N., Zapivakhin, V. O., Komov, S. A., Korotkov, A. A. (2016) O dialektike sderzhivaniia i predotvrashcheniia voennykh konfliktov v informatsionnuiu eru. *Voennaia mysl',* 2016(7), pp 3-11.

Endresen, R. S. (2016) Hard Power in Cyberspace: CNA as a Political Means. In: Pissanidis, N., Rõigas, H. & Veenendaal, M. (eds.) *8th International Conference on Cyber Conflict: Cyber Power.* Tallinn: NATO CCD COE, pp 23-36.

Evans, M. (2005) Elegant irrelevance revisited: A critique of fourth-generation warfare. *Contemporary Security Policy,* 26(2), pp 242-249.
Freedman, L. (2013) *Strategy: A History.* New York: Oxford University Press.

Gerasimov, V. V. (2017) Sovremennye voyny i aktual'nye voprosy oborony strany. *Vestnik Akademii voennykh nauk ,* 59(2), pp 9-13.

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

Gorbachev, Iu. E. (2006) V inostrannykh armiiakh. Setetsentricheskaia voina: mif ili real'nost'?. *Voennaia mysl',* 2006(1), pp 66-76.

Gray, C. S. (1999) *Modern Strategy.* Oxford: Oxford University Press.

Gryzlov, B. M. & Pertsev, A. B. (2015) Informatsionnoe protivoborstvo. Istoriia i sovremennost'. *Vestnik Akademii voennykh nauk,* 51(2), pp 124-128.

Guzzini, S. (1993) The Limits of Neorealist Power Analysis. *International Organization,* 47(3), pp 443 - 478.

Kalinovskii, O. N. (2001) Diskussionnaia tribuna. "Informatsionnaia voina" - eto voina?. *Voennaia Mysl',* 2001(1), pp 57-59.

Karpov, E. A., Burenin, N. I. & Ziuzin, N. A. (2004) Edinoe voennoe informatsionnoe prostranstvo: problemy sozdaniia. *Voennaia mysl',* 2004(8), pp 45-49.

Kartapalov, A. V. (2015) Uroki voennykh konfliktov, perspektivy razvitiia sredstv i sposobov ikh vedeniia. Priamye i nepriamye deistviia v sovremennykh mezhdunarodnykh konfliktakh. *Vestnik Akademii voennykh nauk ,* 51(2), pp 26-36.

Khriapin, A. L. & Afanas'ev, V. A. (2005) Slovo iubiliaram. Kontseptual'nye osnovy strategicheskogo sderzhivaniia. *Voennaia Mysl'*, 2005(1), pp 8-12.

Kirillov, V. V. (2005) Geopolitika i bezopasnost'. Voennaia moshch' gosudarstva: sushchnost', struktura, problemy. *Voennaia mysl',* 2005(9), pp 2-12.

Kokoshin , A. (2007) Asimmetrichnyy otvet nomer odin. *Nezavisimoe Voennoe Obozrenie,* 27 July 2007. [Online] http://nvo.ng.ru/concepts/2007-07-27/4_otvet.*html* [Accessed 4 January 2018]

Kolyvanov, G., 2006. Neponiatnaia asimmeriia. Genshtab popytalsia skazat' novoe slovo v voennoi nauke. *Nezavisimoe Voennoe Obozrenie,* 3 February 2006. [Online] https://dlib.eastview.com/browse/doc/8960544 [Accessed 4 January 2018]

Korytko, V. K. & Sheptura, V. N. (2011) Problemy postroeniia edinogo informatsionnogo prostranstva Vooruzhennykh Sil Rossiiskoi Federatsii i vozmozhnye puti ikh resheniia. *Voennaia mysl',* 2011(10), pp 16-26.

Kukkola, J., Ristolainen, M. & Nikkarila, J-P. (2017) *Game Changer. Structural transformation of cyberspace*. Finnish Defence Research Agency Publications 10. Tampere: Juvenes Print.

Kulakov, A. (2008) Asimmetrichnii otver ne spaset. *Nezavisimoe voennoe obozrenie,* 25 July 2008. [Online] https://dlib.eastview.com/browse/doc/18663911 [Accessed 4 January 2018]

Kuznetsova, N. N. (2013) Ob aktual'nosti problem, sviazannykh s ugrozoi informatsionnoi bezopasnosti. *Vestnik Akademii voennykh nauk,* 44(3), pp 46-47.

Libicki, M. C. (2007) *Conquest in Cyberspace. National Security and Information Warfare.* Cambridge: Cambridge University Press.

Litovkin, V. (2011) Kibervoina s sistemami upravleniia. *Nezavisimoe voennoe obozrenie,* 4 February 2011. [Online] https://dlib.eastview.com/browse/doc/23680274 [Accessed 4 January 2018]

Luttwak, E. N. (2001) *Strategy: The Logic of War and Peace*. Cambridge: The Belknap Press of Harvard University Press.

Matvichuk, V. V. & Khriapin, A. L. (2010) Sistema strategicheskogo sderzhivaniia v novykh usloviiakh. *Voennaia mysl',* 2010(1), pp 11-16.

Mikhailov, N. V. (1999) Vesomye otvety na voyennye vyzovy. *Nezavisimoe Voennoe Obozrenie,* 30 April 1999. [Online] https://dlib.eastview.com/browse/doc/3515343 [Accessed 4 January 2018]

Molchanov, N. A. (2008) Informatsionnyi potentsial zarubezhnykh stran kak istochnik ugroz voennoi bezopasnosti RF. *Voennaia mysl',* 2008(10), pp 2-9.

NVO (2013) Voina v kiberprostranstve: uroki i vyvody dlia Rossii. *Nezavisimoe voennoe obozrenie,* 13 December 2013. [Online] https://dlib.eastview.com/browse/doc/37852459 [Accessed 4 January 2018]

Oehmen, C. & Multari, N. (2014) *AiR: Asymmetry in Resilience: Report on the First Meeting on Asymmetry in Resilience for Complex Cyber Systems.* [Online]
https://cybersecurity.pnnl.gov/documents/AiR_1.0_Final_Report.pdf
[Accessed 19 August 2017]

Orlianskii, V. I. (2008) Informatsionnoe oruzhie i informatsionnaia bor'ba: real'nost i domysly. *Voennaia mysl',* 2008(1), pp 62-70.

Orlianskii, V. I. (2002) Vooruzhennaia i informatsionnaia bor'ba: sushchnost' i vzaimosviaz' poniatii i iavlenii. *Voennaia mysl',* 2002(6), pp. 42-47.

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

Romashkina, N. P. & Koldobskii, A. B. (2015) Novye metody protivoborstva XXI veka. *Vestnik Akademii voennykh nauk,* 50(1), pp 134-139.

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

Sherstiuk, V. P (2003) Aktual'nye problemy obespecheniia informatsionnoi bezopasnosti Rossiyskoi Federatsii. *Voennaia mysl',* 2003(6), pp 28-32.

Sovet Bezopasnosti Rossiiskoi Federatsii (2014) *Zasedanie Soveta Bezopasnosti Rossiiskoi Federatsii po voprosu "O protivodeistvii ugrozam natsional'noi bezopasnosti Rossiiskoi Federatsii v informatsionnoq sfere, 1 oktriabia 2014 goda.* October 1, 2014. [Online]
http://www.scrf.gov.ru/news/allnews/831/ [Accessed 19 December 2017]

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

Strategiia (2009) *O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii do 2020 goda.* [Online]
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102129631 [Accessed 27 September 2017].

Strategiia (2015) *O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii.* [Online]
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102385609 [Accessed 27 September 2017].

Strategiia (2017) *O strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2030 gody* [Online]
http://static.kremlin.ru/media/acts/files/0001201705100002.pdf [Accessed 22 September 2017].

Strel'tsov, A. A. (2011) Osnovnye zadachi gosudarstvennoi politiki v oblasti informatsionnogo protivoborstva. *Voennaia mysl',* 2011(5), pp 18-25.

Thomas, T. (2015) *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics.* Fort Leavenworth: Foreign Military Studies Office.

Tsifrovaia ekonomika (2017) *Programma:"Tsifrovaia ekonomika Rossiiskoi Federatsii".* [Online]
http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf
[Accessed 22 September 2017]

Beprintev, V. B., Manoilo, A. V., Petrenko, A. I. & Frolov, D. B. (2011) *Operatsii informatsionno-psikhologicheckoi voiny: kratkii entsiklopedicheckii slovar'-spravochnik.* Moscow: Goriachaia liniia – Telekom.

Wirtz, J. J. (2017) Life in the "Gray Zone": observations for contemporary strategists. *Defense & Security Analysis,* 33(2), pp 106 - 114.

Vorob'ev, I. N. & Kiselev, V. A. (2014) Kiberprostranstvo kak sfera nepriamogo vooruzhennogo protivoborstva. *Voennaia mysl',* 2014(12), pp 21-28.

Vypasniak, V. I. (2009) O realizatsii setetsentricheskikh printsipov upravleniia silami i sredstvami vooruzhennoi bor'by v operatsiiakh (boevykh deistviiakh). *Voennaia mysl',* 2009(12), pp 23-30.

Yefremov, A. (2017) Formirovanie kontseptsii informatsionnogo suvereniteta gosudarstva. *Pravo. Zhurnal Vysshei shkoly ekonomiki,* 2017(1), pp. 201-205. [Online] https://law-journal.hse.ru/2017--1/204343305.html [Accessed 4 January 2018]

UNDERSTANDING THE GAME BOARD

Civilian and Military Information Infrastructure and the Control of the Russian Segment of the Internet

Juha Kukkola

Abstract

The Russian Federation is constructing the basis for national control of the Internet. This paper provides an overview of the principles and practices of this project and, moreover, examines how Russia implements the concept of 'the unified information space' in building the 'national segment of the Internet.' The main aim of this paper is to find answers to the question as to how Russia is preparing to protect and control its national networks. Specifically, it seeks answers to the question of how 'the unified information space' is structured in civilian and military spheres based on the categories of infrastructure, services, and authorities responsible for creating, monitoring, and controlling this space. This paper argues, firstly, that the distinct Russian idea of 'unified information space' affects the way it strives to shape cyberspace. Secondly, the paper argues that although the national segment of the Internet in Russia has been developed by private actors, it is increasingly subject to centralized civilian and military control. Thirdly, this process is not just about censorship or the control of information, but has a definite military strategic character built into it. This paper provides new information on how Russia is preparing to protect and control its national segment of the Internet and how this may change the military balance in cyberspace.

Keywords: Cyber defence, Civilian and military information infrastructure, Russian Federation, RuNet, Digital sovereignty, Unified information space

The first version of this paper was published and presented at the International Conference on Military Communications and Information Systems (ICMCIS), 22-23 May 2018, Warsaw, Poland.

1 Introduction

The Russian Federation is constructing the basis for national control of the Internet. This is done to protect 'digital sovereignty' (*tsifrovoi suverenitet*). This project has many aspects, one of which is national control over the infrastructure of the Russian segment of the Internet. In the context of 'digital sovereignty' infrastructure can be understood as the physical and logical structure of the Internet, and control as the administrative arrangements to administer this structure. The concept of 'unified information space' (*edinoe informatsionnoe prostranstvo*) (EIP) is critical for understanding this project. It is a strategic cultural concept which has its roots in the Cold War period of history and it shapes current Russian policy. The concept has both a civilian and military component. On the civilian side, control over information and creation of economic benefits are the decisive functions of the concept. On the military side, the control over national infrastructure of the Internet is connected to command and control and its purpose is to provide both a defensive and offensive advantage in cyber space. In this framework, the project of the Russian Federation to control its national network has far ranging strategic implications on the international level.

This paper is built upon and adds to previous studies on the Russian Federation's policies concerning the development of the Internet [1]. The paper provides an overview of the principles and practices behind a Russian project to construct state control over the Internet. Moreover, it examines how Russia implements the concept of 'the unified information space' in building the infrastructure of 'the national segment of the Internet' (*natsional'nyi segment seti "Internet"*). The main aim of this paper is to find answers to the question how Russia is preparing to protect and control its national networks. Specifically, it seeks answers to the question of how 'the unified information space' is structured in civilian and military spheres based on the categories of infrastructure, services, and authorities responsible for creating, monitoring, and controlling this space. In this paper I argue, firstly, that the distinct Russian idea of 'unified information space' affects the way Russia strives to shape cyberspace. Secondly, that although the 'national segment of the Internet' in Russia has been developed by private actors, it is increasingly subject to centralized civilian and military control. Thirdly, this process is not just about censorship or the control of information, but has a definite military strategic character built into it. This paper provides new information on how Russia is preparing to protect and control its national segment of the Internet and how this may change the military balance in cyberspace.

2 Methodology

This paper starts with a conceptual analysis of 'digital sovereignty' and its connection to the idea of 'unified information space'. It then proceeds to analyse how 'the unified information space' is put into practice in civilian and military spheres in building 'the national segment of the Internet'. This analysis concentrates on infrastructure, services, and authorities responsible for them. The paper concludes with a discussion on how the project of creating the 'Russian segment of the Internet' could have a strategic effect at the international level in cyber space. The research material consists of Russian civilian and military academic journals, official documents of Russian authorities, Russian language news articles, and data from institutions following the development of the Internet. Because of the secrecy of the military side of cyberspace, some of the conclusions presented in this paper are inherently speculative.

3 Concepts

Policies of the Russian government on information security have reflected, at least since the beginning of the 2000s, the global trends of globalization and the growth of information society. The main interests of the government have been the enhancement of competitiveness of the domestic digital economy, the protection of information infrastructure and 'spiritual-moral values' (*dukhovno-nravstvennye tsennosti*) from outside interference, and the communication of Russian views to the wider world (i.e. strategic communication). The information space (*informatsionnoe prostranstvo*)[1] has been seen in the context of continuous, albeit fluctuating in intensity, 'counter struggle' (*protivoborstvo*) with the West. According to Russia, in this confrontation the West has had a technological upper hand, it has had a decisive control of the global information space, and it has tried to suppress Russia's great power interests [2], [3].

Behind these policies is the idea that territorial state sovereignty applies to cyberspace, or in the Russian case, to information space. The Russian idea encompasses information infrastructure (technical aspect) as well as information itself (psychological aspect) [4] [3]. This means that the Russian state has the ability, the right and the responsibility to control the national information space, and that any outside infringement may be

[1] "A set of information resources created by the subjects of the information sphere, the means of interaction of such subjects, their information systems and the necessary information infrastructure" [28].

understood as a breach of state sovereignty [5], [6]. Terms used in connection to this concept are 'technological sovereignty' (*tekhnologicheskii suverenitet*) [4], 'information sovereignty' (*informatsionnii suverenitet*) [3], or 'digital sovereignty' (*tsifrovoi suverenitet*) [7]. Currently, this is not how international law defines sovereignty in the information space, but it is how the Russian Federation wants it to be defined [8]. Russia has actively pursued this domestic approach at least since 2014 when it started to develop methods to protect 'the Russian segment of the Internet' and later to create a domestic legal framework for critical information infrastructure and policy for controlling it [9], [10].

The concept of 'unified information space' is critical for understanding how Russians conceptualize 'digital sovereignty'. Officially, it is understood as the aggregate of all information, processes, rules and infrastructure enabling creation, manipulation, transfer, and storage of information [11]. It should not be understood only as information but as a collection of all resources, methods, and processes to create knowledge [12]. The concept has its roots in *kibernetik* thinking of Soviet science from 1960s. Back then, EIP was understood as the unified information network that combined automatized information communication and control systems. On the civilian side it never progressed beyond ideas of controlling the socialist economic system, but on the military side it was developed to the level of a working concept, at least in the case of nuclear weapons command and control (i.e. 'Dead Hand'). [13], [14], [15].

'The unified information space' should be understood as a concept of control of information. The technological aspect of EIP is system-of-systems built upon integrated networks which allows the centralized and hierarchical command and control of national civilian and military assets. On the civilian side it enables communication between various levels of government, provides integrated nation-wide administrative services for federal and local officials and citizens, and additionally, control of the flow of information [16], [17]. The infrastructural part of EIP is recognized in Russian law as the Unified Telecommunication Network of the Russian Federation which includes public, dedicated, technological, and special purpose networks [18].

On the military side EIP enables aggregated and automatic command and control of military assets through information [19] [20]. It provides the armed forces' primary and secondary networks of communication, and aggregation and distribution of information to create situation awareness [21]. Based on the ideas presented by Russian writers, it can be argued that

EIP is the combination of principles of Network Centric Warfare – which Russians have been studying from the beginning of the 2000s [22] – and Russian historical strategic cultural ideas – hierarchical and centralized command[2] – and geographical realities of the Russian Federation.

Both the civilian and military sides of EIP are required in the building of 'the Russian segment of the Internet' and to protect this entity from outside threats.

4 Civilian Infrastructure and Services

The development of the infrastructure of the Russian segment of the Internet has been driven by civilian and commercial actors and interests [23] [24]. In 2014 the Russian government took a decidedly more active role by revising its program for developing the information society from 2010. The current program has been updated several times [25], [26]. In 2017 Russia also updated its strategy for the development of the information society from 2008 [27], [28]. The main motives behind this change were: the acknowledgement that Russia still relied heavily on legacy networks which led to 'digital inequality' (*tsifrovogo neravenstvo*); backwardness of Russia's digital economy; and monitoring of and defending against information threats. The project is aimed at the totality of infrastructure of the national segment of the Internet, and Russian language Internet services and community, commonly known as 'RuNet.'

4.1 Infrastructure and services of RuNet

Currently, RuNet is built on the physical backbone connections provided mainly by five companies (Rostelekom, MTS, Vimpelkom, MegaFon, and TransTeleKom). Optical fibre connects the main population centres, but microwave and satellite connections are important as well as cellular networks, and there are hundreds of ISPs running networks and services although many are local [29], [30], [31]. Provider networks are connected on the data link layer by internet traffic exchange points (IXPs); the two biggest are MSK-IX (38 nodes with over 500 customer Autonomic Systems [AS]) and DataIX (18 nodes with over 150 customer ASs) [32] [33]. IXP infrastructure is mostly situated in the western part of Russia or along the Siberian railway route [34] and routing between ASs is done by BGP4 [35].

[2] This characteristic is made visible in the current Russian military reform which strives to move away from rigid hierarchy in command and control [98]. This idea is also present in the Information security doctrine [3].

There are ca. 11 root-level DNS in Russia. Rostelekom controls MSK-IX which is responsible for top-level domain name servers for .ru and .pф domains. It has nodes in 7 federal okrugs (i.e. districts) and abroad [36]. Rostelekom is also the national registry operator [37] and operates the AS which has the most connections to neighbours of Russia [38].

There have been plans since 2012 to expand the infrastructure of RuNet to a network between BRICS countries by building an undersea cable exclusively between them although this project seems to have stalled [39], [40]. Additionally, the Commonwealth of Independent States has adopted a declaration to create a 'unified information space.' This project too has faced difficulties and is very much incomplete [41]. Moreover, Russia is planning to clone OneWeb LEO -satellite project to provide Internet regionally and globally to 'friendly' countries [42].

RuNet is characterized by domestic, Russian language services such as search engines (Yandex), social network sites (Vkontakte, Odnoklassiki, LiveJournal) and email services (mail.ru). These are services provided by private companies but the companies themselves are connected to political power through oligarchy, state programs, and the good will of political leadership [43]. In fact, the government has an intense interest in promoting the Russian language content and cultural homogeneity of RuNet [10]. Additionally, domestic digital services, products and technological solutions are perceived to have a major positive effect on the economic development of the Russian Federation in times of Western sanctions and heighted competition [28]. The creation of a digital economy interconnects authoritarian political and economic interests, and societal control as one of the building blocks of 'digital sovereignty' [17].

Alongside the public Internet, the national segment also includes other networks. One is the Russian State Network (RSNet). It is defined as a segment of the Internet designated for the use of Russian federal organizations and federal subjects and is based on the gov.ru domain. It consists of systems, networks, and computers which are operated by the Federal Protective Service (FSO). RSNet is connected to the Internet through a gateway and has its own IP-address space and DNS system. It provides users with email and other services. It can be described as the Russian Federation's internal administrative network. [44]. At least part of the traffic of RSNet is conducted through a 'Unified data network' (*Edinoi seti peredachi dannykh* - ESPD) [45]. A reason behind creating RSNet was to provide a single, secure gateway to the Internet for government organizations [46]. It is also elemental part of Russian eGovernment which is based on Unified portal of state services (*Edinoi portal gosuslug*) and

Unified system of identification and authentication (*Edinaia sistema identifikatsii i autentifikatsii*) i.e. electronic citizenship [47]. The system already has 50 million registered users [48].

Connected to RSNet, but still a distinct concept, are the special purpose networks, or closed government networks. They are meant for government organizations, defence, security of state, and ensuring law and order [18].

4.2 Control and protection of the national segment of the Internet

The concept of 'the Russian national segment of the Internet' is important for understanding how the 'unified information space' and 'digital sovereignty' mesh under state control and protection. It is defined in a law draft by Minkomsviaz' (Ministry of Telecommunications and Mass Communications) as: "a set of information and communication networks, systems, and Internet resources located on the territory of the Russian Federation and registered in accordance with the established procedure in compliance with the legislation of the Russian Federation and the national domain zone .ru, .рф, as well as resources assigned to the national segment of the Russian Federation on the basis of relevant international treaties" [49]. This national segment is mentioned, but not defined in any approved official documents.

Connected to 'the national segment of the Internet' is critical (information) infrastructure (CII). Minkomsviaz's law draft defines critical infrastructure of the Internet as networks, systems, and resources that affect information infrastructure of the national segment of the Internet. From this definition are derived the components of critical infrastructure which are the national domain zone .ru, .рф and the infrastructure providing its functioning: IXPs, GosSOPKA (cf. below), and the infrastructure of autonomous systems[3]. This infrastructure is sometimes called GIS "Internet" (*Gosudarstvennaia Informatsionnaia Sistema "Internet"*) [50]. In contrast to the law draft, the Russian government has already enacted a law that gives a basic definition of CII (information systems, networks, and automatized control systems in the services of critical services of society). It gives the state the right to determine which elements of infrastructure are critical, and therefore, control over private CII. The service providers are given the responsibility to implement the protection of CII [51].

[3] Autonomous system implicitly refers to autonomous system number used by Border Gateway Protocol (BGP) [99].

In fact, the main backbone connections are already controlled by the state-owned Rostelekom [52]. To strengthen this control Minkomsviaz' is proposing that ISPs must observe regulations when establishing connections over state borders, that foreign ownership of IXPs should be restricted, and that all ISPs must connect their networks to registered IXPs [49]. Additionally, Minkomsviaz' has plans to duplicate critical components of CII in the name of national security [53].[4] Overall, ISPs are quite strictly regulated by Minkomsviaz', The Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) and Federal Security Service (FSB) [51] [54].

Since 2013 the Russian state has implemented a variety of laws that have imposed restrictions on the freedom of RuNet [10]. These include filtering of illegal traffic and black listing which are delegated to the responsibility of ISPs. Additionally, government has the SORM-3 (*Sistema Operativno-Rozysknykh Meropriiatii*) system for monitoring and intercepting traffic [55]. SORM-3, as are many other instruments of Internet control, is based on a Russian version of Public Private Partnership (PPP) where government tries through legal measures to coerce the private sector to implement measures and to pay for them [23]. This has led to haphazard and ineffectual implementation [56]. Monitoring and censorship measures are derived mainly from political interest and from efforts to fight cybercrime. They target the content of traffic and are aimed at maintaining the political stability of the Russian Federation [54]. This is understandable because information infrastructure, and with it, Internet penetration among the population has been growing fast (ca. 73% in 2017) [54], [30], [31].

For a variety of reasons, the monitoring, controlling and protecting of the public side of RuNet has been distributed to multiple actors. Currently, a collection of CERTs (RU-CERT, GOV-CERT, FinCERT) are monitoring different networks [56]. This challenge of disunity was implicitly noted in the Russian government's program on 'Digital economy' (2017), as a task to create a centre for securing a 'unified network of electronic communications' in Russia [7].

The GosSOPKA (*Dosudartsvennia Sistema obnaruzheniia, preduprezdeniia i likvidatsii posledsvii komp'iuternykh atak*) is an answer to this challenge. It is defined as "[…] a single territorially distributed

[4] Critical components in this context are understood as IANA managed root zone file of DNS root servers, RIPE NCC registry of IP -addresses, and RIPE NCC routing registry [100].

complex, including forces and means designed to detect, prevent and eliminate the consequences of computer attacks and respond to computer incidents" [51]. The project of building GosSOPKA was initiated in 2013 by president Vladimir Putin [57]. It has been envisioned as a centrally controlled territorial system. The FSB has had the preliminary role as an administrator and standardiser of the system, and private companies are involved in developing it. GosSOPKA should be used by all state organizations and by private ISPs managing information infrastructure deemed as critical. It is intended to monitor network attacks, alert management, and provide defensive measures [58], [59], [60].

4.3 The securitization of RuNet

The tendencies to unify and centralize communication, services, and security in RuNet are apparent in the strategies and programs approved by the Russian state in 2016-2017 and are reflected by the development of the Russian segment of the Internet described above. As the Information doctrine of the Russian Federation clearly states, information security (widely understood as psychological and technological) is part of strategic deterrence, and a part of that is protection of critical information infrastructure. The undisturbed functioning of information infrastructure is one of Russia's national interests [3]. This objective is secured by "the unity of state regulation, centralized monitoring and management of the functioning of the information infrastructure of the Russian Federation at the level of information systems and data processing centres, and also at the level of communication networks" [28]. This concept includes domestic encryption solutions, national certification of software and hardware, and advancing domestic production of information technology [28]. Measures to secure RuNet are trained annually in a joint exercise by Minkomsviaz', FSB and the Ministry of Defence (MoD) [61]. The ultimate manifestation of this tendency to protect 'the national segment of the Internet' is the project to ensure its continuous functionality by duplicating its critical components and by achieving the capability to partly or completely disconnect it from the larger Internet [62]. This can be argued to be both a defensive and offensive measure [1].

5 Military Infrastructure and Services

The Russian armed forces claim to have their own 'military Internet' i.e. 'closed data segment' (*Zakrytii segment peredachi dannykh*) which was declared operational in 2016 [63]. The infrastructure is partly leased from Rostelekom and partly based on the infrastructure of the MoD. Military

units have their own servers and routers which encrypt information and transmit it using packet-based protocol. The network is air-gapped from the Internet and hosts are special workstations certified and controlled by the MoD. Use of flash drives is restricted. The 'Military Internet' has its own second and third level DNS domains (domain.mil.zs) [63]. It is possible that the operating system, at least on a tactical level, is Astra Linux [64] and some of the hardware is based on Russian components manufactured by Voentelekom [65]. The main provider of communication and control systems to the armed forces is United Instrument Manufacturing Corporation (under state corporation Rostek) which includes for example Central Research Institute of Economics, Informatics and Control Systems (TSNII EISU). TSNII EISU is the direct descendant of the institution which developed automated command and control systems in Soviet times [66].

In addition to leased capacity, the communication infrastructure of the armed forces is based on optic fibre, satellite, and microwave relay networks operated by the MoD. By 2017 T8 corporation claims to have laid 67 000 km of fibre optic cable of which 15 000 km is based on 100 Gbits DWDM system "Volga" [67]. Additionally, Voentelekom has laid 200 km of fibre optic cable during 2007-2017. The corporation is partly responsible for building communications between security institutions, military-technological industry, and critical infrastructure [68]. Communication satellites are necessary for military communications because Russian geography does not allow for nationwide fibre connections. The Russian military operates its own satellite fleet which consists of at least thirty 'store-and-dumb' communication satellites and approximately twenty-seven GLONASS -navigation satellites. The armed forces probably also use commercial SATCOM satellites [69]. Interestingly, there is a concept of 'unified cosmic system' (*Edinaia Kosmicheskaia Sistema*) which refers to a missile early warning system [70]. The Russian military also uses terrestrial radio relay links on HF/UHF/SHF frequencies which provide varied data transmission capacity [71]. Because of the multiplicity of systems and legacy systems, armed forces communications may not be as efficient as Russian commercial systems, but there is still a clear interest in maintaining a distinct military data network.

It is probable that this 'military Internet' is physically and / or logically distinct from the communication network used by nuclear forces for obvious security reasons. Additionally, there are other branch and service specific networks that require special gateways for connection to the 'unified information space' [72]. There is also a partly completed project to create a common air defence network between states belonging to the Commonwealth of Independent States (CIS) [73]. Additionally, the

Collective Security Cooperation Organization (CSTO) has adopted a resolution to enhance common information (technical and psychological) security [74]. These projects create an interesting element within the military 'unified information space' where allied nations are incorporated into the Russian information space. To protect Russian national networks, it is possible that these connections are implemented through controlled gateways. On the cross-sectoral side, Voentelekom has been constructing separate network for the needs of the Military industrial complex (MiC). This should combine MiC with ministries, agencies and armed forces during peace time and in crisis situations [75].

The 'Military Internet' may enable the 'Joint automated digital communication system' (*Ob"edinennaia avtomatizirovannaia tsifrovaia sistema svyazi - OATsSS*) of the Russian armed forces. This system provides automated command and control of communications and automated command and control of forces [76]. It may provide centralized command and control of forces from the MoD, through military districts down to army level, and decentralized control of networks. It is part of the effort of the Russian armed forces to homogenize communication and command and control systems of the armed forces. The concept divides networks into backbone, access, and local networks which should be able to support different command and control systems of services and branches. Moreover, in the spirit of total defence, the networks should support other security services [76].

In the centre of OATsSS is the National Defence Management Centre in Moscow which was established in 2014. The Centre combines information flows from multiple military and governmental sources (networks) to create a common situational picture. It has its own super computer to assist in automation of command and control [77]. In the timeframe of 2015-2018 similar command centres are planned to be established at branch and service headquarters, military districts and major tactical formations [78].

It should be noted that a 'unified automatized command and control system' is not a new concept for the Russian military. The idea was already developed during the 1980s but remained underdeveloped and was fragmented to various branch specific systems [21]. Compared to the United States armed forces' concept of 'military Internet' the clear difference is that the Russian approach is more rooted in the idea of total defence where all state security organizations are connected by the same network and command and control system [79]. It should be noted that progression of this idea to reality has been anything but simple because of

the multiplicity of branch and service specific systems and legacy solutions [80].

6 Authorities and Responsibilities

An important aspect of 'the unified information space' is who controls it and how. In Table I actors and responsibilities are shown in the framework of different elements of RuNet.

The Security Council of the Russian Federation has a significant role in formulating Internet-related strategies and policies. These are implemented after approval by Minkomsviaz' which also administers, monitors, and regulates networks through its subordinates. In practice, the security services have a significant role in all aspects of controlling and protecting the 'national segment of the Internet.' The FSB coordinates the actions of public and private security actors concerning cyber security, counter-intelligence etc. The FSB also controls encryption algorithms and licensing together with FSTEK. Although, security services have a significant role in controlling RuNet, private actors play a significant role in providing connectivity, security, and services. The military operates its own networks and the military's relationship to other controlling actors is a bit ambivalent.

It is quite clear that there are some over-lapping functions which may hinder creation, control, and monitoring of EIP. Multiple actors are responsible for monitoring and security of 'the national segment of the Internet.' Licensing is distributed among many actors. Laws and policies are drafted by different institutions and the concept of critical information infrastructure has muddled the borders between private and public spheres. Considering relations presented in Table I, it might be too early to speak about EIP as an existing structure. Nevertheless, there is a technological and political unifying process which intertwines actors vertically and horizontally through Russian government and society.

Table I[5]
RuNet: Actors, Elements and Responsibilities

Actors	Networks					
	Public RuNet	***RSNet***	***Closed government networks***	***Military internet***	***Critical information infrastructure***	***Corporate networks***
Security Council [81]	SP DLP	SP DLP	SP DLP	SP DLP	SP DLP	SP DLP
Minkomsviazi [82], [83]	PC DLP LR	PC DLP LR	PC DLP LR	DLP LR	PC DLP LR	PC DLP LR
Rozkomnadzor [84]	ACS M	ACS M				ACS M
Rossviaz' [85]	R M	R M	R			R M
Rospechat' [86]	C	C	C			C
Ministry of Defence [63]				A S,M,C CO		
Federal Security Service (FSB) [51], [57], [87]	LE, DLP S,M,C E, L	S,M,C E, L	S,M,C E, L		DLP S,M,C E, L	LE E, L
Federal Protective Service (FSO) [88]		R, M A, S	R, M A, S			
The Federal Service for Technical and Export Control (FSTEK) [89] [90]	L CE	L CE	L CE	L E, CE	L,A,R CE	L CE
Computer Emergency Response Teams [91] [92] [93]	S(a) M	S(b) M	S(b) M	S(c) M	S(d) M	S (d&e) M
Military Industial Complex [75], [94]				CO SER	A SER	A SER
Internet Service Providers [95] [68]	CO SER	CO SER	CO SER	CO SER	CO SER	CO SER
Private companies [96], [97]	SER	SER	SER	SER	SER SEC	A SEC SER

[5] Abbreviations: Law enforcement (LE), Security (S) – RU-CERT(a), GOV-CERT(b), Military SOCs (c), CERT-GIB / Private SOCs (d), FIN-CERT (e), Monitoring (M), Coordination (C), Cryptography (E), Licensing (L), Regulation (R), Administration (A), Certification (CE), Strategic planning (SP), Drafting laws and policies (DLP), Connectivity (CO), Services (SER), Political control (PC), Legal regulation (LR), Administrative control and supervision (ACS). FSB (Federal Security Service), FSO (Federal Protective Services), FSTEK (Federal Service for Technical and Export Control), SCRF (Security Council), MoD (Ministry of Defence), MIC (Military Industrial Complex), Minkom. (Minkomsviaz'), Roskom. (The Federal Service for Supervision of Communications, Information Technology and Mass Media), CERT (Computer Emergency Response Team), ISP (Internet Service Provider), Rossviaz' (Federal Communications Agency – under Minkomzvazi), Rospechat' (Federal Agency for Press and Mass Communications - under Minkomzvazi), Private (Civilian private sector including state corporations)

7 Discussion

Russia prepares to protect and control its national networks by creating a 'unified information space' that is centrally controlled by the state. This concept is apparent both in the civilian and military domain. There is a tension between, on the one hand, the global connectivity necessary for power projection, the need to extend EIP over borders to allies, and economic development and, and on the other hand, the territorial concept of an information space. The driving principle is horizontal unification and vertical control of networks. The idea is not only to control the freedom of information but to control cyberspace for political, security and economic purposes. Centralization of control and monitoring is paramount, although lip-service is paid to individual rights and freedoms in official documents. In contrast to this drive to centralize, is the delegation and dispersion of responsibilities to different state organizations. Organizations themselves have hierarchical command structures but the information space has no single controlling institution. This phenomenon reflects the Russian Federation's overall security structure where many actors (FSB, MoD, National guard etc.) are responsible for the security of the state. There are also a variety of public and private organizations in the information space which have been developed to manage the security of information services and traffic in the absence of state control. This constellation, with its contradictions, is the product of the interaction of free and uncontrolled development and deeply ingrained, resurgent strategic cultural ideas.

The government of the Russian Federation sees the development of the information society both as an opportunity and a risk, and the idea of 'digital sovereignty' reflects this. Risks are clear. They are connected to outside interference and internal instability. Opportunities are connected to the possibility to achieve through closed national systems and markets a Russian hardware and software version of the Internet. This would provide a new national source of income when energy prices fluctuate, or oil and gas deposits eventually run dry or become too expensive to exploit. It could create a platform for a Russian 'Silicon Valley' and open export markets in countries which do not trust Western or Chinese products. Additionally, technological and administrative solutions behind 'digital sovereignty' may provide Russia a unified, resilient and deeply protected national segment of the Internet which can be disconnected from the global Internet at will. At the same time, Russia would be free to take advantage of the vulnerabilities of other nations. This would have far ranging strategic implications on the international level. It should shape our thinking on such issues as deterrence, resilience, and escalation control in cyberspace.

Acknowledgment

I would like to thank Mari Ristolainen for her invaluable support and insight that greatly assisted in the writing of this paper.

References

[1] J. Kukkola, M. Ristolainen & J.-P. Nikkarila, *Game Changer. Structural transformation of cyberspace*, Riihimäki: Finnish Defence Research Agency, 2017.

[2] *Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii,* Pr-1895 (2000, Sep. 9). [Online]. Available: http://base.garant.ru/182535/#ixzz4x5P8ZYEp. [Accessed 31 October 2017].

[3] *Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii*, Ukaz Presidenta RF N 646 (2016, Dec. 5). [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf. [Accessed 2017 September 22].

[4] *Osnovy gosudarstvennoi politiki Rossiyskoi Federatsii v oblasti mezhdunarodnoi informatsionnoi bezopasnosti na period do 2020 goda*, Pr-1753 (2013, Jul. 24). [Online]. Available: https://xn--b1aew.xn--p1ai/upload/site1/document_file/Osnovy_gospolitiki_v_oblasti_mezhd_inf_bezopasnosti.pdf. [Accessed 31 October 2017].

[5] V. E. Makarov, *Politicheskie i sotsial'nie aspekti informatsionnoi bezopasnosti*, Moscow: S. A. Stupin, 2015.

[6] A. A. Efremov, ”Formirovanie kontseptsii informatsionnogo suvereniteta gosudarstva,” *Zhurnal Vysshei shkoly ekonomiki*, no. 1, pp. 201-215, 2017.

[7] *Programma “Tsifrovaia ekonomika Rossiiskoi Federatsii”* No 1632-p (2017, Jul. 28). [Online]. Available: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf. [Accessed 22 September 2017].

[8] M. Schmitt and L. Vihul, *International Cyber Law Politicized: The UN GGE’s Failure to Advance Cyber Norms, Just Security*, (2017, Jun. 30). [Online]. Available: https://www.justsecurity.org/42768/international-

cyber-law-politicized-gges-failure-advance-cyber-norms. [Accessed 19 August 2017].

[9] Sovet Bezopasnosti Rossiiskoi Federatsii, “O protivodeistvii ugrozam natsional’noi bezopasnosti Rossiiskoi Federatsii v informatsionnoi sfere”, (2014, Oct. 1). [Online]. Available: http://www.scrf.gov.ru/news/allnews/831/. [Accessed: 23 January 2018]

[10] M. Ristolainen, ”Should ‘RuNet 2020’ Be Taken Seriously? Contradictory Views about Cyber Security Between Russia and the West,” *Journal of Information Warfare*, vol. 16, no. 4, pp. 113-131, 2017.

[11] Kontseptsiia formirovaniia i razvitiia edinovo informatsionnovo prostranstva Rossii i sootvetctviushchikh gosudarstvennykh informatsionnykh resursov, Pr-1694 (1995, Nov. 23). [Online]. Available: http://lawru.info/dok/1995/11/23/n453820.htm. [Accessed 10 January 2018].

[12] A. V. Manoilo, A. I. Petrenko and D. B. Frolov, *Gosudarstvennaia informatsionnaia politika v usloviakh informatsionna-psikhologicheskikh konfliktov vysokoi intensivnosti i sotsial'noi opasnosti*, (3rd ed.), Moscow: Goryachaya liniya - Telekom, 2013.

[13] V. V. Baraniuk, ”Edinoe informatsionnoe prostranstvo VS RF: problemy sozdaniia,” *Voennaia mysl'*, vol. 2003, no. 003, pp. 36-38, 2003.

[14] B. Peters, *How Not to Netwok a Nation: The Uneasy History of the Soviet Internet*, The MIT Press: Cambrige, 2016.

[15] J. G. Hines, E. M. Mishulovich and J. F. Shull, *Soviet Intentions 1965-1985: Volume II Soviet Post-Cold War Testimonial Evidence*, BMD Federal Inc, McLean, 1995.

[16] Prikaz Federal’noi sluzby okhranii “Ob utberzdenii Polozeniia o rossiiskom gosudarstvennom segmente informatsionno-telekommunikatsionnoi seti "Internet" 7.9.2016 No 443.” [Online]. Available: http://publication.pravo.gov.ru/Document/View/0001201610170008?index=0&rangeSize=1. [Accessed 10 January 2018].

[17] V. V. Bukharin, ”Komponenty tsifrovogo suvereniteta Rossiiskoi Federatsii kak tekhnicheskaia osnova informatsionnoi bezopasnosti,” *Vestnik MGIMO-Universiteta*, vol. 6, no. 51, pp. 76-91, 2016.

[18] Federal’nyi zakon O zviazi ot 07.07.2003, N 126-F3 (red. ot. 05.12.2017). [Online]. Available: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=284294&fld=134&dst=417,0&rnd=0.1557327116187115#0. [Accessed 11 January 2018].

[19] E. A. Karpov, N. I. Burenin and N. A. Ziuzin, ”Edinoe voennoe informatsionnoe prostranstvo: problemy sozdaniia,” *Voennaia mysl'*, Vol. 2004, no. 008, pp. 45-49, 2004.

[20] V. K. Kopytko and V. N. Sheptura, ”Problemy postroeniia edinogo informatsionnogo prostranstva Vooruzhennykh Sil Rossiiskoi Federatsii i vozmozhnye puti ikh resheniia,” *Voennaia mysl'*, vol. 2011, no. 10, pp. 16-26, 2011.

[21] A. P. Tolmachev, V. V. Baraniuk and N. N. Tiutiunnikov, ”Informatsionnoe obespechenie upravleniia Vooruzhennymi Silami Rossiyskoi Federatsii,” *Vestnik Akademii voennykh nauk*, vol. 36, no. 3, pp. 102-105, 2011.

[22] T. Bukkvoll, ”Iron Cannot Fight – The Role of Technology in Current Russian Military Theory,” *Journal of Strategic Studies*, vol. 34, no. 5, pp. 681-706, 2011.

[23] A. Soldatov and I. Borogan, *The Red Web. The Struggle Between Russia's Digital Dictators and The New Online Revolutionaries*, New York: Public Affairs, 2015.

[24] A. Soldatov, ”The Taming of the Internet,” *Russian Social Science Review*, vol. 58, no. 1, pp. 39-59, 2017.

[25] Rasporiazenie Pravitel’ctvo Rossiiskoi Federatsii “O gosudarstvennoi programme Rossiikoi Federatsii "Informatsionnoe obshchestvo (2011-2020 gody)" 20.10.2010 N 1815-p.” [Online]. Available: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102349623&backlink=1&&nd=102142714. [Accessed 10 January 2018].

[26] Postanovlenie pravitel’ctvo Rossiiskoi Federatsii ”Ob utverzdenii gosydarstvennoi programmy Rossiiskoi Federatsii "Informatsionnoe obshchectvo (2011-2020 gody) 15.4.2014 N 313." [Online]. Available: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102142714&backlink=1&&nd=102349623 . [Accessed 10 January 2018].

[27] *Strategiia razvitiia informatsionnogo obshchectba v Rossiiskoi Federatsii,* Pr-212 (2008, Feb. 20). [Online]. Available: https://rg.ru/2008/02/16/informacia-strategia-dok.html. [Accessed 10 January 2018].

[28] Ukaz presidenta Rossiiskoi Federatsii “O strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2030 gody 9.5.2017 No 203.” [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf. [Accessed Accessed 22 September 2017].

[29] Minkomsviaz', ”Godovoi otchet o khode realizatsii i otsenke effektivnosti gosudarstvennoi programmy Rossiiskoi Federatsii "Informatsionnoe obshchestvo (2011-2020 gody)",” (2017, Apr. 4). [Online]. Available: http://minsvyaz.ru/ru/documents/5551/. [Accessed 21 January 2018].

[30] Rospechat', ”Internet v Rossii v 2016 gody - sostoianie, tendentsii i perspektivy razvitiia,” Rospechat, Moscow, 2017. [Online]. Available: http://raec.ru/upload/files/171220-rif-report-2017.pdf. [Accessed: 24 January 2018]

[31] RAEK, ”Tsifrovaja ekonomika 2016 - Ezegodnoe obshchrossiiskoe issledovanie otchestvennogo rynka vysokikh tekhnologii,” RAEK, Moscow, 2017. [Online]. Available: http://files.runet-id.com/2016/presentation-research/presentations/itogy2016-booklet.pdf. [Accessed: 24 January 2018]

[32] MSK-IX, ”MSK-IX,” 2018. [Online]. Available: https://www.msk-ix.ru. [Accessed 10 January 2018].

[33] DATAIX, “DATAIX,” 2018. [Online]. Available: http://dataix.ru/partnership/. [Accessed 10 January 2018].

[34] Rostelekom, ”Magistral'naia set' sviazi,” 2018. [Online]. Available: https://www.rostelecom.ru/about/net/magistr/. [Accessed 21 January 2018].

[35] BGP View, ”Countries report - Russia,” 2018. [Online]. Available: https://bgpview.io/ix/73. [Accessed 21 January 2018].

[36] Root-servers.org, ”Root-servers.org” 2018. [Online]. Available: http://www.rootservers. [Accessed 10 January 2018].

[37] A. Balashova and Petr Kanaev “”Rostelekom” stal operatorom reestra domenov .ru and .pф,” RBK, (2018, Jan. 23).

[38] IDIDB “Runet connectivity” (24.1.2018). [Online]. Available: http://www.ididb.ru/en/runet/bgp.html [Accessed 24 January 2018].

[39] S. Lee, ”International Reactions to U.S. Cybersecurity Policy: The BRICS undersea cable,” Henry M. Jackson School of International Studies, Washington, 2016.

[40] E. Trifonova, ”Rossiia predlozila razdelit' Internet: Na iuridicheckom forume BRICS ideiia nezavicimoi Seti obcuzdalac' v kontekste bor'by s kiberugrozami,” *Nezavizimaia gazeta*, (2017, Dec. 1).

[41] I. V. Surma, ”Edinoe informatsionnoe prostranstvo SNG: 20 let spustia,” *Voprosy bezopasnosti*, vol. 2015, no. 5, pp. 41-58, 2015.

[42] A. Balashova , I. Sidorkova and Mariia Kolomychenko, ”Pravitel'ctvu predlozat sozdat' global'nuiu set' za R299 mlrd,” *RBC*, (2017, Nov. 22).

[43] E. Osetinskaya, ”Yandex, a Russian Success Story and Putin’s High-Tech Tiger (Op-ed),” *The Moscow Times*, (2017, Sep. 27).

[44] Government of Russian Federation, ”Vremennye pravila administrirovaniia domena gov.ru,” 2018. [Online]. Available: http://www.gov.ru/main/rsnet/page541.html. [Accessed 11 January 2018].

[45] Minkomsvyaz, ”Edinuiu set' peredachi dannykh v 2016 godu budut ispol'zovat' 14 gosorganov,” Minkomsvyaz, 2016. [Online]. Available: http://minsvyaz.ru/ru/events/34535/ [Accessed 24 January 2018].

[46] Tadviser, ”RSNet Russian State Network Set' dlia gosstruktur,” 2017. [Online]. Available: http://tadviser.ru/a/53423. [Accessed 1 November 2017].

[47] Minkomsviaz, “Edinaia sistema identifikatsii i autentifikatsii - Rukovodstvo operatora tsentra obsluzhivaniia ESIA verija 2.7, Minkomsviaz,” 2017. [Online] Available: http://minsvyaz.ru/uploaded/presentations/rukovodstvooperatoratsov27.pdf [Accessed 24 January 2018].

[48] Minkomsviaz, ”Pochti 53 mln grazhdan Rossii imeiut vozmozhnost′ pol′zovat′sia elektronnymi gosuslugami,” (2017, Aug. 14). [Online]. Available: http://minsvyaz.ru/ru/events/37267/. [Accessed 17 November 2017].

[49] Minkomsvyaz, ”Federal'nyi zakon «O vnesenii izmenenii v Federal'nii zakon «O svyazi» (Proekt),” (2017, Aug. 15). [Online]. Available: http://regulation.gov.ru/projects#npa=71277. [Accessed 1 November 2017].

[50] M. Kolomychenko, ”GIS "Internet" prosit perezagruzki: Vlasti ishchut dengi na bezopasnost' rossiiskogo segmenta seti,” *Kommersant*, (2017, Feb. 3).

[51] Federal'nyi zakon O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii ot 26.7.2017 N 187-FZ. [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_220885/. [Accessed 1 November 2017].

[52] Rostelekom, ”Universal'nye uslugi sviazi i proekt ustarennia tsifrovogo neravnstva,” 2018. [Online]. Available: https://www.rostelecom.ru/projects/uus/. [Accessed 10 January 2018].

[53] A. Balashova and M. Kolomychenko, ”Vlasti predlozhili novye ogranicheniia dlia vladel'tsev tochek obmena trafikom,” *RBK*, (2017, Aug. 16).

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

[55] K. Ermoshina and F. Musiani, ”Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet,” *Media and Communication*, vol. 5, no 1, pp. 42-53, 2017.

[56] M. Kolomychenko and A. Makhukova, ”Vne proslushki: pochemu Roskomnadzor i FSB sudiatsia s operatorami sviazi,” *RBK*, (2017, Nov. 9).

[57] *Vybiska iz Kontseptsii gosydarstvennoi sistemy obnaryzeniia, preduprezdeniia i likvidatsii posledstvii komp'iuternykh atak na informatsionnye resursy Rossiiskoi Federatsii*, No K 1274 (2014, Dec. 12). [Online]. Available: http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf. [Accessed 10 January 2018].

[58] Solar Security, ”Reshenie po cozdaniiu tsentrov GosSOPKA ot Solar JSOC,” 2017. [Online]. Available: https://solarsecurity.ru/upload/pdf/Solar_JSOC_GOSSOPKA.pdf. [Accessed 24 January 2018].

[59] V. Driukov, ”GosSOPKA: to, o chem obychno molchat - Zadachi operatsionnoi bezopasnosti ob'ektov KII v ramkakh funktsionirovaniia tsentrov GosSOPKA: to, chto zabyvaiut skazat',” *Voenno-promyshlennyi kyr'er*, (2017, Dec. 5).

[60] K. Zukova, ”GosSOPKA sdadut pod kliuch: Solar Security i Positive Technologies zaimutcia sozdaniem tsentrov kiberbezopasnosti,” *Kommersant*, (2017, Nov. 11).

[61] TASS, ”Glava Minkomsviazi poobeshchal provodit′ ezhegodnye ucheniia po obespecheniiu ustoichivosti runeta,” *TASS*, (2014, Nov. 19). [Online]. Available http://tass.ru/obschestvo/1582671 [Accessed: 24 January 2018]

[62] A. Rezchikov, ”Izbezat' otkiucheniia ot interneta Rossii pomozet Kitai,” *Vzgliad*, (2016, Dec. 29).

[63] V. Zykov and R. Aleksey, ”V Rossii poiavilsia voennii internet Zakrytii segment peredachi dannykh pozvoliaet podrazdeleniiam Minoborony bezopasno obmenivat'sia sekretnoi informatsiei,” *Izvestiia*, (2016, Oct. 19).

[64] N. Grishchenko, ”Rossiiskie voennye sozdali sobstvennyi internet,” *Rossiiskaia gazeta*, (2016, Oct. 19).

[65] Zvezda, ”Voennyi Internet: kak rabotaiut zakrytye tekhnologii ministerstva oborony,” *Zvezda*, (2017, Apr. 9). [Online] Available https://tvzvezda.ru/news/vstrane_i_mire/content/201704091018-4ygi.htm [Accessed 24 January 2018]

[66] A. Ramm, ”Na ostrie ekonomiki i avtomatizatsii - Unikal′nomu nauchno-issledovatel′skomu institutu ekonomiki, informatiki i sistem upravleniia ispolniaetsia 45 let,” *Voenno-promyshlennyi kur'er*, vol. 19, no 537, 2014, pp. 9.

[67] M. A. Sleptsov, ”DWDM-sistemy sviazi dlia Vooruzhennykh sil,” in *Tematicheskii sbornik «Sviaz' v Vooruzhënnykh Silakh Rossiiskoi Federatsii — 2017»,* Moscow: Informatsionnyi Most, 2017, pp. 124.

[68] O. Vladykin, ”Voentelekom obecpechit cilobikov cpetssviaz'iu: Postroeno dopolnitel'no okolo 200 km optovolokonnykh linii,” *Nezavizimoe voennoe obozrenie*, (2017, Feb. 17).

[69] Union of Concerned Scientists, ”UCS Satellite Database,” 2017. [Online]. Available: http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.Wg0WlUpl9PY. [Accessed 16 November 2017].

[70] K. Riabov, ”Ob”iavleno o nachale stroitel′stva Edinoi kosmicheskoi sistemy,” *Nezavizimoe voennoe obozrenie*, (2014, Oct. 13).

[71] V. A. Maliukov, ”Sovremennym voiskam - sovremennuiu sviaz′,” in *Sviaz' v Vooruzhennykh Silakh Rossiiskoi Federatsii — 2013*, Moscow: Informatsionnyi Most, 2013, pp. 14-16.

[72] V. Lanchev, ”ASU VKO: model′ dlia sborki Uchebnye komandnye punkty dolzhny lech′ v osnovu podgotovki spetsialistov VKO,” *Voenno-promyshlennyi kur'er*, vol. 39, no. 605, 2015, pp. 5.

[73] G. Plopsky, ”Russia’s Big Plans for Air Defense in Eurasia: Big plans, indeed, but will they materialize?,” *The Diplomat* (2017, Apr, 7). [Online]. Available: https://thediplomat.com/2017/04/russias-big-plans-for-air-defense-in-eurasia/. [Accessed 11 January 2018].

[74] P. P. Riabukhina, V. V. Bondurovskogo and G. I. Perek, *Zakonodatel'stvo gosudarstv — chlenov Organizatsii Dogovora o kollektivnoi bezopasnosti v sfere obespecheniia informatsionnoi bezopasnosti: opyt, problemy i perspektivy garmonizatsii*, Saint Petersburg: Parlamentskia assambleia organizatsii dogovora o kollektivnoi bezopasnosti, 2014.

[75] A. Pan'shin, ”Glava "Voentelekoma": tekhnologiia blokchein mozet poiavit'cia v armii Rossii,” *Voentelekom*, (2017, Aug. 22). [Online]. Available: https://voentelecom.ru/news/novosti-kompanii/glava-voentelekoma-tekhnologiya-blokcheyn-mozhet-poyavitsya-v-armii-rossii/. [Accessed 11 January 2018].

[76] K. Arslanov and A. Likhachev, ”Aktual'nye nauchno prakticheskie problemy razvitiia OATsSS VS RF,” in *Sviaz' v Vooruzhennykh Silakh Rossiyskoi Federatsii — 2015*, Moscow: Informatsionnii Most, 2015, pp. 29-36.

[77] I. Gavrilov, ”Glava Genshtaba ob”iasnil, kak budet rabotat′ Tsentr upravleniia oboronoi,” *Rossiiskaia gazeta*, (2014, Nov 1).

[78] A. V. Khomutov, ”Opyt i perspektivy ispol'zovaniia kontseptsii edinoi informatsionno-kommunikatsionnoi seti v upravlenii voiskami,” *Voennaia mysl'*, vol. 2015, no 11, 2015, pp. 17-22.

[79] USMilcom, ”USMilcom,” 2014. [Online]. Available: http://www.usmilcom.com/military.htm. [Accessed 1 November 2017].

[80] V. Ivanov, ”Porshnevoe upravlenie - Ctoby dostich′ proryva v razrabotke mezhvidovoi ASU, Minoborony dolzhno sdelat′ stavku ne na kustarei, a na gosudarstvennikov,” *Voenno-promyshlennyi kur'er*, vol. 33, no 599, 2015, pp. 8.

[81] Federal'nyi zakon O bezopasnosti 28.12.2010 N 390-F3 (red. ot 05.10.2015),”. [Online]. Available: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=187049&fld=134&dst=100086,0&rnd=0.24186836654385746#0. [Accessed 11 January 2018].

[82] Postonovlenie pravitel’stvo Rossiiskoi Federatsii “O Ministerctve sviazi i massovykh kommunikatsii 02.07.2008 No 418 (red. ot 01.07.2016).” [Online]. Available: http://minsvyaz.ru/uploaded/files/polozhenie-o-ministerstve-svyazi-i-massovyih-kommunikatsij-rossijskoj-federatsii.pdf. [Accessed 11 January 2018].

[83] Minkomzviaz', ”Opublikovan zakonoprojekt ob obecpechenii ustoichivosti rossiiskogo segmenta seti "Internet",” (2016, Nov. 10). [Online]. Available: http://minsvyaz.ru/ru/events/36040/. [Accessed 1 11 2018].

[84] Postonovlenie pravitel’stvo Rossiiskoi Federatsii “O Federal'noi sluz'be po nadzory v sfere sviazi, informatsionnykh tekhnologii i massobykh kommunikatsii 16.03.2009 N 228 (red. ot 01.07.2016).” [Online]. Available: https://rkn.gov.ru/about/p179/. [Accessed 11 January 2018].

[85] Postanovlenie pravitel’stvo Rossiiskoi Federatsii "Ob utverzdenii Polozeniia o Federalnom agenstve sviazi» 20.6.2004 No. 320.” [Online]. Available: http://base.garant.ru/187177/. [Accessed 22 January 2018].

[86] Postanovlenie pravitel'ctva Rossiiskoi Federatsii "O Federal'nom agenctve po pechati i massovym kommunikatsiiam 17.6.2004 No. 292.” [Online]. Available: http://base.garant.ru/187125/. [Accessed 22 January 2018].

[87] Prikaz Federal’noi sluzby okhranii No. 41821, (2016, Apr. 18). [Online]. Available: http://www.fsb.ru/files/PDF/prikaz_182.pdf. [Accessed 11 January 2018].

[88] Ukaz presidenta Rossiiskoi Federatsii “O nekotorykh voprosakh informatsionnoi bezopasnosti Rossiiskoi Federatsii 22.5.2015 No. 260.” [Online]. Available: http://publication.pravo.gov.ru/Document/View/0001201505220028. [Accessed 11 January 2018].

[89] FSTEK, ”Svedeniia o polnomochiiakh FSTEK Rossii; perechen' normativnykh provovykh aktov, opredeliaiushchikh eti polnomochiia,” (2016, Mar. 28). [Online]. Available: http://fstec.ru/obshchaya-informatsiya/polnomochiya. [Accessed 11 January 2018].

[90] Prikaz FSTEK “Ob utverzdenii trebovanii k obespecheniiu zashchity informatsii v avtomatizirovannykh sistemakh upravleniia proizvodcvenniymi i tekhnologicheckimi protsessami na kritichecki vaznykh ob"ektakh 14.3.2014 N 31 (red. ot 23.3.2017)” 14 March 2014. [Online]. Available: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31. [Accessed 11 January 2018].

[91] GOV-CERT.ru, ”Informatsiia o GOV-CERT.RU,” 2018.[Online]. Available: http://www.gov-cert.ru/. [Accessed 11 January 2018].

[92] RU-CERT.ru, ”Tsentr reagirovaniia na komp'iuternye intsidentiy,” 2018. [Online]. Available: https://www.cert.ru/ru/about.shtml. [Accessed 11 January 2018].

[93] FinCERT.ru, 2018. [Online]. Available: https://www.cbr.ru/fincert/. [Accessed 11 January 2018].

[94] Voentelekom, ”Voentelekom prinial uchastie v podgotovke k strategicheskim ucheniiam "Zapad-2017",” (2017, Aug. 11). [Online]. Available: https://voentelecom.ru/news/novosti-kompanii/voentelekom-prinyal-uchastie-v-podgotovke-k-strategicheskim-ucheniyam-zapad-2017-/. [Accessed 11 January 2018].

[95] Provy.ru, 2018. [Online]. Available: http://russia.provy.ru/providers. [Accessed 10 January 2018].

[96] A. N. Bobkov, S. V. Tsibin and I. A. Bystrov, *Sviaz' v Booryzenniykh Silakh Rossiiskoi Federatsii - 2017*, Moscow: Informatsionnyi Most, 2017.

[97] Minkomzviaz', ”Nikolay Nikiforov Presented Branch Plan on Import Substitution of Software,” (2015, Apr. 3). [Online]. Available: http://minsvyaz.ru/en/events/32967/. [Accessed 12 January 2018].

[98] T. Thomas, *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics*, Fort Leavenworth: Foreign Military Studies Office, 2015.

[99] J. Hawkinson, ”RFC 1939 Guidelines for creation, selection, and registration of an Autonomous System (AS),” March 1996. [Online]. Available: https://tools.ietf.org/html/rfc1930. [Accessed 10 January 2018].

[100] A. Sukharevskaia and I. Iuzbekova, ”Lishnego ne utechet: Kak imenno chinoviki namereny obezopasit' Runet,” *RBC*, (2016, Jun. 17).

Projected Territoriality: A Case Study of the Infrastructure of Russian Digital Borders

Juha Kukkola
Mari Ristolainen

Abstract

Territoriality is increasingly projected into cyberspace. The Russian Federation is constructing the infrastructural basis for national control of the Internet. This is done to ensure 'digital sovereignty'. A 'digital border' is a key concept for ensuring 'digital sovereignty'. Therefore, in order to ensure Russian 'digital sovereignty' the 'digital borders' of a national segment of the Internet need to be firstly, delineated; secondly, protected; and thirdly, cross-border control needs to be organized. This article is a case study of the delineation, protection and control processes of Russian 'digital borders'. Moreover, this article represents an original attempt to demonstrate how territoriality can be projected into cyberspace on the level of infrastructure of an individual country. We argue that by using delineation, protection, and control as analytical concepts to study national ideas about and practical efforts to build 'digital borders' and 'digital sovereignty' it is possible to gain a comparative perspective of how geographic territory is projected to cyberspace through governmental control of specific elements of cyberspace. We describe how 'digital borders' are constructed through the vertical and horizontal combination of authorities and infrastructure within the Russian national segment of the Internet. These 'digital borders' could ensure undisturbed functioning of this national segment which could be considered as a certain model for future 'digital border security', i.e. a form of cyber security. By combining Border studies, Information technology studies and Russian studies this article provides an interdisciplinary overview of the infrastructure of the Russian segment of the Internet, and examines the principles and practice behind the Russian implementation of the concept of the 'national segment of the Internet' as an infrastructural part of delineating 'digital borders' and achieving a functional 'digital sovereignty'. This article improves understanding of diverse approaches to cyber security, national security policies, as well as, bringing a new insight to an infrastructural basis of a national segment of the Internet.

Keywords: Cyber Security, National Security Policy, Russia, National Segment of the Internet, Critical Information Infrastructure, Digital Sovereignty, Digital Borders

The first version of this paper was published and presented at the 17th European Conference on Cyber Warfare and Security (ECCWS), 28-29 June 2018, Oslo, Norway. The second version of this paper was published in the Journal of Information Warfare 2018, 17.2, pp. 83-100.

1 Introduction

Territoriality is increasingly projected into cyberspace. The Russian Federation is constructing the infrastructural basis for national control of the Internet. This process is explicitly connected to the concept of digital sovereignty. Russian academics have been discussing legal aspects of state sovereignty in the context of information space since at least 1999 (Efremov 2017, pp. 209-210). Yet the concept of sovereignty in the information space (*suverenitet v informatsionnom prostranstve*) was first officially mentioned in the Information Security doctrine (Doktrina 2016) where the task to ensure the protection of the sovereignty of the Russian Federation in the information space is considered the main direction of information security in the sphere of strategic stability and equitable strategic partnership (see, for example, Bukharin 2016, p. 77; Pilyugin 2017, p. 38). This official recognition and the policy following it can be attributed to Russia´s interest in subjugating the Internet to national control of sovereign states and denying technologically more advanced states an advantage against Russia in information space (United Nations 2011 & 2015). It needs to be noted that, in the Russian language, 'cyberspace' is called 'information space'. The Russian concept of information space includes all mass media, not only information and computer technology platforms (Doktrina 2016). This article uses the term 'information space' when referring to the Russian understanding of cyberspace.

Russia is actively pursuing this policy through its Strategy on the Development of an Information Society in the Russian Federation for 2017-2030 (Strategiia 2017) which states that the Russian segment of the Internet (*rossiiskii segment seti 'Internet'*) must be nationally controlled, independent, self-sufficient, protected from outside interference, and under sovereign jurisdiction. Despite being a central concept for the strategy, the concepts of a Russian segment of the Internet, or its analogue a national segment of the Internet (*natsional'nyi segment seti 'Internet'*), are not clearly defined in Russian official publications. Additionally, some

Russian academics use the term ‘Russian segment of cyberspace’. A practical realisation of the strategy, the state program called the ‘Digital Economy of the Russian Federation’ (Programma 2017) presents a road map tasking that Russia will be digitally sovereign by 2020. Additionally, another state program called ‘Digital Information Society 2011-2020’ states that Internet providers should be fully controlled by state regulation and that 99% of Internet resources should be registered by 2020 (Kantyshev & Golits'na 2016).

Digital sovereignty requires digital borders to mark the limits of state jurisdiction and power. Therefore, to ensure Russian digital sovereignty, the digital borders of a national segment of the Internet need to be delineated and protected, and cross-border control needs to be organised. By combining border studies, information technology studies, and Russian studies, this article provides an interdisciplinary overview of the infrastructure of the Russian segment of the Internet and discusses how it reflects the ‘digital border’ formation processes. As a research design, the authors have chosen an exploratory case study. Exploratory case studies investigate a distinct phenomenon characterised by a lack of detailed preliminary research (Yin 2009). The scope of this article is limited to Russia and to Russian concepts. The authors’ aim is solely to analyse the Russian understanding of digital sovereignty and digital border-making practices. The aim is to provide an in-depth analysis and to gain a comparative perspective of how territoriality can be projected into cyberspace at the level of infrastructure of an individual country. Moreover, the authors try to provide a conceptual toolbox on how to study border-making practices in cyberspace in the future.

This article starts with conceptual definitions of state, sovereignty, territoriality, and borders in the physical-geographical space and then it introduces concepts of delineation, protection, and control for studying these phenomena. Next, it explains how border concepts could be applied in cyberspace. It then applies the aforementioned concepts regarding the Russian concept of digital border in more detail. It then demonstrates how the process of developing digital borders is progressing in Russia; how borders in cyberspace could be delineated and protected; and how the cross-border traffic of a national segment could be controlled. Finally, it shows how these processes combine into a system-of-systems that forms the infrastructural basis of digital borders and digital sovereignty. The research material used consists of previous Russian border and cyber studies, official Russian government documents, Russian language news articles, and data from institutions following the development of the Internet.

2 State, Sovereignty, Territoriality, and Borders

There are several different definitions of state, sovereignty, territoriality, and borders depending on the authors' background (for example, political geography, political science, international relations, sociology, history, and anthropology). These definitions reflect different perspectives on the Westphalian state system, where each nation state has sovereignty over its territory.

The authors define a state as a society that has a legitimate monopoly on sovereign political power and legal jurisdiction within the territorial limits of a given society (see Kireev 2015). Sovereignty is understood as the rule of state power over this society in relation to any other power. Territoriality limits the state's sovereignty within a certain territory. A state border is an establishment of the spatial limits of a sovereign state that ensures the authoritative regulation of cross border relations (Kireev 2015, pp. 99-100). A legitimate state's border depends on international legal recognition and its geographical location with respect to bordering states.

Put simply, for a state border to be legitimate, it needs to be clearly delineated and protected; and the control of cross-border traffic must be organized (see Kudinov 2014; Tsarenkova 2016; Kireev 2015). International boundary making is a specific legal process that consists of detailed stages, such as (border) treaties, delimitation, and demarcation (see Adler 2001). These stages have largely established and internationally shared content and meanings. Delimitation is conventional international legal recognition and registration of the state border by which two sovereign nations establish and describe in writing the location of their common boundary, mainly as the output of the decision making on the negotiation table (Introduction to Border Studies 2015 s.v. delimitation). Demarcation is a field operation and a process of exact fixation, marking, and logging of location of the line of state border established by the delimitation agreements (Introduction to Border Studies 2015 s.v. demarcation).

After a state border is legally established, the next step is to organise its protection. Border protection is typically a mission of specialised institutions, for example, by a border control agency. Furthermore, border control or related security institutions are given the power to control cross-border relations and to organise and to regulate cross-border traffic. In the case of Russia, a branch of the Federal Security Service of Russia (FSB), the Border Service of the Federal Security Service of the Russian

Federation (*Pogranichnaia sluzhba Federal'noi sluzhby besopasnosti Rossiiskoi Federatsii*), is tasked with guarding the Russian state border. Yet, the internal structure of any modern state border protection and control system is very complex and heterogeneous. To comprehend the complexity of this structure, it is crucial to examine the specific components of a state border system—including the formal roles and institutions and how they are linked in different structures and activities.

Cyberspace represents a novel, man-made, imaginary, malleable, and transitory space that is radically different from physical-geographical space (see Libicki 2009; Choucri 2012; Sheldon 2013). Thus, the first challenge is to develop suitable concepts for border-making practices in cyberspace and then to understand what kinds of institutions, structures, and activities could be involved in the state border system of cyberspace. In the authors' opinion, the delineation, protection, and cross-border control practices of border making in the physical-geographical space are good starting points for the study of border-making practices in cyberspace.

3 Applying Border Concepts in Cyberspace

Cyberspace has been envisioned as a space where borders and states are no longer able to adapt in the Westphalian state system (Tuukkanen 2013; Nocetti 2015). Nevertheless, the Russian concept of 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, pp. 113-114; Kukkola, Ristolainen & Nikkarila 2017). These findings seem to be consistent with what Demchak and Dombrowski (2013) have called a Cyber Westphalia, such as the territorialisation of cyberspace. This means the end of a frontier period for the Internet, during which interstate order is established in cyberspace. This process requires states to build institutions, to establish authorities and agreements, and to prepare for possible confrontations with other states.

However, applying border-making practices to cyberspace is somewhat challenging as the entire concept of border is confusing in borderless cyberspace. There is no common or academic understanding as to what borders in cyberspace are or even what concept to use (such as cyber border, virtual border, unspatialised border, or iBorder, for example). In this article, the authors apply the concept of 'digital border', primarily because it is a direct translation of a concept used in Russian (*tsifrovaia granitsa*) and also because the word 'digital' refers to computer technology

and data processing. When speaking about establishing borders in cyberspace, the authors use the English verb 'delineate'. 'Delineate' captures the specificity of border making in cyberspace better than the verb 'demarcate', which is linked to the actual physical border-marking practices in physical-geographical space. Moreover, 'delineation' also suggests the graphical or mathematical representation of a border in physical-geographical space. Furthermore, a digital border is a key concept for ensuring digital sovereignty (*tsifrovoi suverenitet*).

Based upon the authors' analysis, a digital border represents an entity that separates potential national segments of cyberspace from other similar segments. These segments are primarily understood as parts of the Internet (consisting of content and infrastructure), but also include other networks under national jurisdiction or located on sovereign territory. Nevertheless, border making presupposes prior common and shared space, so it is possible to concentrate on open networks, such as the Internet, and apply the official Russian term 'national segment of the Internet'.

Established digital borders are only judicial concepts that do not guarantee security or autonomy (excluding total disconnection). To ensure digital sovereignty, these borders must be protected. In cyberspace, this could be done through various technological means, institutions, information sharing, and agreements. Protection is facilitated by control, which means actors with authority and means to monitor and, if necessary, to intervene and to investigate illegitimate cross-border and internal traffic. Only through protected and controlled borders in cyberspace, however defined or constructed, can digital sovereignty be established in the national segment of the Internet.

Building borders in cyberspace is a form of governance by infrastructure. From this viewpoint, borders are not something that exist independently, but are a product of different forms of intentional design and administration of technologies and enactment of policies (DeNardis 2014). These technologies and policies must be combined in a system of systems—a set of different systems so connected or related as to produce results unachievable by the individual systems alone, if digital borders are to be effective (Krygiel 1999, pp. 33-34).

3.1 Digital sovereignty (*tsifrovoi suverenitet*)

The legal aspects of state sovereignty in information space have been discussed in Russia since 1999 (Efremov 2017, p. 209). Some scholars claim that digital sovereignty as a concept has been part of the Russian

information space discussion and research starting from 2012 (Dubov 2014, p. 125; Nocetti 2015, p. 113). One of the main visionaries behind the concept is an Internet Technologies (IT) expert, Igor Ashmanov (2013), who envisions digital sovereignty as a right and an ability of the national government to independently determine geopolitical national interests in the digital environment. Polikarpov and Polikarpova (2014) follow Ashmanov's ideas and see information sovereignty as an integral part of Russian state sovereignty that, according to them, is threatened by the development of modern information technology.

Vladislav Bukharin (2016) connects sovereignty explicitly to ownership and implicitly to authority when listing several technical components of digital sovereignty. According to Bukharin (2016), the technical components of Russian digital sovereignty are: (1) search engines; (2) social media; (3) domestic operating systems and software; (4) microelectronics; (5) networking equipment; (6) national segment of the Internet; (7) payment systems; (8) self-protection; (9) cryptographic algorithms and protocols; and (10) navigation systems. Bukharin (2016) does not connect digital sovereignty to the state's ruling power over its information space but to the state's ownership of the technical components.

Alexey Efremov (2016, pp. 55-56) discusses the legal problems of the realisation of state sovereignty when (physical) territory changes into (information) space. He argues that state sovereignty may decrease in this process, but also that the denotation of sovereignty changes from territorial to functional in the information space. According to Efremov (2017, p. 211), the key aspect in the realisation of state sovereignty in information space is the state's ability to regulate information connections (*informatsionnye otnosheniia*) in the information space. Efremov (2017) defines state sovereignty in the information space as the state's ability to regulate certain information space by implementing national (domestic) laws together with international legislation that has been formed together with the state in question.

When summarising Russian academic discussions on the aspects of sovereignty in the information space, it is clear that most of them are not focused on the practical or technical side of the realisation of 'digital sovereignty'. Anatoly Streltsov and Pavel Pilyugin (2016) take a significantly different approach to digital sovereignty when they explain their view on the main components of 'digital sovereignty'. Their article represents the first Russian open-source scientific study on how to achieve digital sovereignty in practice. Streltsov and Pilyugin (2016, pp. 28-29) give the technical parameters of how to maintain a nationally governed

network and suggest that digital sovereignty requires the delineating of cyberspace, such as the formation of 'digital state borders'.

Based on Russian writers and official documents, digital sovereignty is understood in this article as the extension of the authority and control of a territorial state to the national segment of the Internet, which consists of Internet and other network related ICT systems located on its territory or under its jurisdiction. A wider concept is information sovereignty, which includes the information residing or flowing through those ICT systems and the interaction of its users.

3.2 Digital border (*tsifrovaia granitsa*)

Streltsov and Pilyugin (2016) explain how there are certain rules regarding how national borders are to be protected and how different subjects cross national borders (for example, border-making processes in the physical-geographical space). Similarly, they argue that border crossing should be organised through virtual digital border crossing points where the incoming/outgoing (cross-border) traffic can be monitored. Moreover, they introduce the concept of digital customs (*tsifrovaia tamozhnia*). Digital customs enforcement would not check all the information packets passing through the digital border, but would have a right to monitor the so-called "legitimacy of the information flow" (Streltsov & Pilyugin 2016, p. 28). For information security reasons, all of the programs used should be certified by national certification organisations. The national operators (providers) would be able to organise the traffic, but they would be under the control and supervision of the state. According to Streltsov & Pilyugin (2016, p. 29), all of this could be organised with existing technology by using Border Gateway Protocol (BGP), a standardised exterior gateway protocol designed for exchanging routing and reachability information among Autonomous Systems (AS) on the Internet. Together with innovative use of Software Defined Networking (SDN) technology, states would be able to form their own policies and reach international or bilateral agreements for their digital border crossing.

Pavel Pilyugin (2017) has developed these ideas further and argues that there are at least four potential ways to delineate borders in cyberspace. Borders can be delineated by controlling real objects in the physical world (such as the end devices and their interaction with cyberspace) or by controlling the data flow at the intersection of the physical border (such as the Great Firewall of China). According to Pilyugin (2017, p. 38-39), these two approaches are not cost-effective solutions. The third option Pilyugin (2017, p. 39) examines is based on IP addresses, but he concludes that

borders cannot be based on monitoring and controlling of traffic that cannot be reliably associated with a specific source or destination. Pilyugin's (2017, p. 40) fourth option is based on BGP which would combine physical control (traffic-exchange points, cross-border connections, and juridical or human owners) to control traffic (Autonomous System based routing). BGP could be used to control traffic inside and even outside the national segment of the Internet. He adds to this option technological and informational control, which basically means using registration of traffic at the border and inside the national network, using layered firewalls, and monitoring content. Pilyugin (2017, p. 40) further proposes using SDN to centrally control this system on a national level.

Pilyugin (2017, p. 42-43) concludes by presenting a three-tier model on how to delineate, protect, and control digital borders. It is on national-level firewall control; SDN controllers, which transmit data on traffic and topology to a command centre and enable routing, filtering, and control of traffic and real-time situation awareness; and on Software Defined Internet Exchange Points, which create one national AS and allow national-level BGP control. Pilyugin (2017) proposes multi-layered control of traffic and content, which is based on nationally controlled BGP routing and is built upon governmentally controlled SDN. As Pilyugin (2017) hints, this solution could be used to manipulate traffic on the wider Internet and form a basis for an alternative Internet based on territorially defined cyberspace regulated through bi- or multi-lateral agreements.

4 Delineation of Russian Digital Borders in Cyberspace

The Russian Federation has approached the delineation of cyberspace from two directions. The first is connected to the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, such as the UN GGE process (see Tikk 2017), and the second to national policy formulation and law-making (Osnovy 2013). Both are connected to the concept of a national segment of the Internet, which has appeared in Russian international treaties, national security documents, and government programs (CSTO 2014; Doktrina 2016; Programma 2017).

Since 1998 Russia has tried through international norm building to get other states (at least other great powers) to recognise state control of the Internet (Dylevskii *et al.* 2007). Acceptance would, in effect, project territorial state sovereignty into cyberspace because it involves the

recognition of rights and responsibilities of states over their information space and critical information infrastructure (United Nations 2015). Borders would be delineated along information space and critical information infrastructure. The Russian-led proposal also insists on the responsibility of states to secure the Internet but, to prevent outside intervention in the case of perceived failure, frames this as an equal, multilateral and transparent effort (United Nations 2015; Tikk 2017).

The Russian government began actively to delineate national borders in cyberspace after 2014 (Roskomsvoboda 2017). Before this, it concentrated on the larger 'information space' which included mass media, spiritual values, and the digital economy (for example, see Strategiia 2009; Kontseptsiia 2013). The central concept around which borders are being defined is information infrastructure. This is a collection of networks and systems, including the Internet, which is situated on Russian territory, territory under Russian jurisdiction, or which is used by the Russian federation according to international treaties (Doktrina 2016). A subcomponent of this collection is Critical Information Infrastructure (CII), which is basically defined as a state interest and put under state jurisdiction through a national law (Federal'nyi zakon 2017a). A second central concept is information space which appeared as early as the Information Security doctrine of 2000 (Doktrina 2000), but really gained traction in the Military doctrine of 2014 (Doktrina 2014). The doctrine connected information space to military threats and so, implicitly, to sovereignty. The Information Security doctrine of 2016 went a step further and mentioned 'the protection of sovereignty of the Russian Federation in information space' (Doktrina 2016). Later, a government program for the digital economy set as a target for 2020 to "secure digital sovereignty of the Russian Federation" (*obespetsen tsifrovoi suverenitet Rossiiskoi Federatsii*) (Programma 2017, p. 20). Alongside these strategic documents, Russia has between 2011-2017 approved a group of laws that have given the state broad powers to monitor and to control information in the Russian Internet, and to restrict foreign ownership of information infrastructure and information distribution (see Freedom House 2017).

Although there are no official definitions of digital borders in Russian public documents, the idea of delineation is present. Borders are delineated through international, if need be bi- or multi-lateral agreements, through territorial state control of information infrastructure, by securing information space, and through national laws. The borders have territorial, judicial, economic, cultural, and military characteristics.

5 Protection of Russian 'Digital Borders' in Cyberspace

Because the establishment of digital borders is ongoing, their protection is somewhat difficult to distinguish from delineation and control. Nevertheless, protection seems to concentrate on the CII of the national segment of the Internet. To establish points of traffic across digital borders, to restrict traffic through anywhere else, and to protect this arrangement, the Russian government has sought to give CII a legal status and has designated the responsibility for its protection to security services and private companies (Federal'nyi zakon 2017a). The government has also sought to restrict traffic to designated Internet Exchange Points (IXPs) and has sought to ensure domestic ownership of these entities (Minkomsviaz 2017). Additionally, data traffic through these points should be transparent and should be conducted in ways that can be monitored by, *inter alia,* security services (Federal'nyi zakon 2017b). This arrangement, in effect, creates a protection procedure that is connected to physical, territorial infrastructure. Responsibility for the procedure is given to the private sector, supervised by the security services.

Additionally, Russia has approved laws requiring localisation of personal data and data retention. These require the creation of huge national data centres and restrict the movement of data outside Russia (Federal'nyi zakon 2017c). In a way, this 'data sovereignty' will form a part of digital sovereignty (Efremov 2017). Data location and its protection define digital borders. Additionally, the government has a project to 'duplicate' critical services, specifically to acquire national copies of IANA managed root zone file of DNS root servers, RIPE NCC registry of IP addresses, and RIPE NCC routing registry (Roskomsvoboda 2017). These should enable the functioning of the Russian segment of the Internet even if it is disconnected from the outside (Sukharevskaia & Iuzbekova 2016). Alongside this 'duplication' project, the Russian government is trying to restrict 99% of domestic Internet traffic inside Russian borders (Kantyshev & Golits'na 2016). These projects form a basis for protecting digital borders from the inside out in the absence of international agreements regarding how national segments of the Internet and state rights to protect their borders should be defined.

The government programs for the digital economy and information society (Programma 2014; Programma 2017) are also efforts to protect digital borders: by establishing registries of forbidden sites and responsibilities on blocking traffic to those sites and by establishing domestic hardware and

software development and production to secure national, technological control of CII. The protection of Russian digital borders is being developed mainly by the regulation on CII and data and through technological projects to ensure resiliency of these borders and their control by authorities, with the help of the private sector.

6 Control of Russian 'Digital Borders' in Cyberspace

Because international agreements are lacking, controlling cross-border traffic has been approached by the Russian state from the inside out. The first part of this approach is to limit and control outside information flows and the ownership of CII through laws (Federal'nyi zakon 2017a). This might seem like state censorship, but it also serves to define what kind of traffic is allowed through Russian digital borders and how. Laws also regulate whose traffic is allowed through borders from the outside (Federal'nyi zakon 2017c; Federal'nyi zakon 2017d). There is a tendency in these laws to strive for a peculiar kind of Russian Public Private Partnership (PPP) in which the state orders private companies to monitor illegal traffic, to protect their networks, to pay for this protection, and to consent to state control of these protection mechanisms (cf. Federal'nyi zakon 2017a). Russia has enforced the above mentioned laws by, for example, banning or restricting the operations of international social media companies (Freedom House 2017).

The second part of this protection consists of the systems created to monitor traffic and the information infrastructure. Russia's SORM-3 (*Sistema Operativno-Rozysknykh Meropriiatii*) system is part of this, but it is meant for capturing small amounts of traffic, and there are reservations regarding how effective this system is because it is paid for and maintained by private actors. (Kolomychenko & Makhukova 2017). Russia has a group of national level Computer Emergency Response Teams (CERTs), but these rely mainly on information sharing and cooperation with public and private institutions, which are responsible for protecting their own networks (International Telecommunication Union (ITU) 2015). On the content side, Internet Service Providers (ISPs) are responsible for monitoring websites and must restrict access to sources declared illegitimate by *Rozkomnadzor* (the federal service for supervision of communications, information technology, and mass media). This system is bureaucratic and reactive (Golunov, Gorbachev & Turovskii 2017). To make the situation even worse from the point of view of digital borders, Russia's information infrastructure has been developed by various private actors without much

regulation on how to connect their backbones to networks outside Russian territory (Pilyugin 2017).

The system called GosSOPKA (*Gosudarstvennaia sistema obnaruzheniia, preduprezhdeniia i likvidatsii posledsvii komp'iuternykh atak*) is partly an answer to challenges described above. It has been defined as "a single territorially distributed complex, including forces and means designed to detect, prevent and eliminate the consequences of computer attacks and respond to computer incidents" (Federal'nyi zakon 2017a, p. 3). The system would have regional centres and one national centre to aggregate all data and to respond to incidents, and it would be administered by the security services. GosSOPKA is still in the development phase (Zukova 2017), but it could become the government's horizontally integrated and vertically administered system for controlling cross-border traffic.

Controlling cross-border traffic cannot rely only on regulation or technological systems. Control of digital borders is also a state function; and, in Russia, that is done through a variety of government ministries and agencies. The Security Council of the Russian Federation has a significant role in formulating Internet-related strategies and policies (SCRF 2017). These are partly implemented by *Minkomsviaz* (the Ministry of Communications and Mass Media of the Russian Federation), which mainly regulates public and private actors and has outsourced much of its control function to different agencies or even to private firms. *Minkomsviaz* is also the main responsible actor in developing the digital economy and society, which implicitly means control over borders of those entities (Programma 2014).

Rozkomnadzor, in principle, controls and supervises Russia's national Internet; but in practice, the Federal Security Service (FSB) and, to a lesser extent, the Federal Protective Service (FSO), play a significant role in monitoring traffic and enforcing norms (including controlling SORM-3 and GosSOPKA). The FSB also controls encryption algorithms and licensing, which is closely connected to sovereign control of information because it enables the monitoring of the content of cross-border traffic (Polozhenie 2016; Prikaz 2016a; Prikaz 2016b; Ukaz 2015). The Federal Service for Technical and Export Control (FSTEK) has a similar role concerning equipment and technologies (FSTEK 2016). The FSB also coordinates the actions of public and private security actors concerning cyber security and counter-intelligence (Ermoshina & Musiani 2017; Soldatov 2017). Although security services play a significant role in controlling the national segment of the Internet, private actors play a role in providing connectivity, security, and services. It must be kept in mind

that ‘private’ also includes state corporations such as Rostelekom. This means that a significant part of Russia’s CII is, in fact, controlled by the state (Rostelekom 2018a & 2018b; Pan’shin 2017). Altogether, a close reading of the law drafts, strategies, doctrines, and government programs make it clear that security agencies and, to lesser extent, *Minkomsviaz* have recently gained decisively more control over information infrastructure, traffic, and its content (see Federal’nyi zakon 2017a & 2017b; Programma 2014; Doktrina 2016; Programma 2017; RSPP 2017).

Although control mechanisms are being developed, there are some overlapping functions, and perhaps interagency rivalries, which may hinder the cross-border control of digital borders. Nevertheless, there is a clear effort to control the digital borders of the national segment of the Internet by the Russian state. This control relies on the cooperation of the private sector but is definitely under state jurisdiction and is achieved through centralised monitoring systems.

7 Digital Borders as a System-Of-Systems

When the technologies and policies of delineation, protection, and control presented above are viewed separately, the picture can seem a bit chaotic and incoherent. But these technologies and policies can also be viewed as subsystems of a system-of-systems that provides the basis for digital borders and eventually for digital sovereignty. This holistic view shows that the Russians might be pursuing a unified information space, which basically means a horizontally integrated and centrally controlled national information network (Kukkola 2018c).

The first subsystem is composed of administrative and technical measures to remove and restrict access to unwanted content on the Internet, including the banning of foreign Internet services. Additionally, there are efforts to remove anonymity from the Russian Internet by restricting the use of Virtual Private Networks (VPNs) and by introducing digital identification. The function of this system is the control of traffic and the control of traffic traceability (Federal’nyi zakon 2017b; Kukkola 2018b). The second subsystem consists of a targeted surveillance system (SORM) and massive Internet data traffic retention by ISPs. These enable traffic and content-based analysis of security threats and appropriate actions by security services. The function of this system is the control of the content of traffic (Soldatov 2017). The third subsystem is based on domestic encryption solutions. The system’s primary function is to achieve internal security through transparency—security services that might have access to

backdoors and encryption keys of domestic products (Programma 2017; Kukkola 2018b). The fourth subsystem is a nation-wide, state-led information infrastructure project that could provide Internet to remote areas. Infrastructure will be owned by state-controlled companies, and it is reasonable to expect that the architecture built by these companies will serve the strategic interests of the state. The function of this system is to allow the state to control the routes of cross-border and internal traffic (Plan 2018; Roskomsvoboda 2018).

The fifth subsystem is based on state control of Critical Information Infrastructure (CII) through laws and state ownership. This system's function is to protect CII but also to give the state indirect or direct control of cross-border traffic exchange points (Federal'nyi zakon 2017a; Postanovlenie 2018). The sixth subsystem consists of a network of national SIEM (Security Incident and Event Management) systems and a network of national CERTs. The system will be deployed in public and corporate networks. Its function is to enable a national, centrally and vertically controlled system of monitoring, incident management, and response for the national segment of the Internet (Kukkola 2018b & 2018a). The seventh subsystem consists of state control of Internet traffic routing on the physical and logical levels, which aims to create a basis for a separated and, if needed, a closed Russian segment of the Internet. Its function is to enable the closing of digital borders, if necessary.

If the Russian government manages to combine the above-mentioned subsystems into a system-of-systems, it will gain centralised control of the national digital borders. This capability will, among other things, significantly enhance the concept of digital sovereignty. Delineation, protection, and control are combined in a way not unlike those presented by Streltsov and Pilyagin (2016). This system could provide a blueprint for similar efforts to build borders in cyberspace.

8 Conclusions

Is the Russian Federation truly pursuing digital sovereignty by establishing digital borders? Based on the analysis of the writings of Russian academics and official government documents, it appears that it is. Academic ideas may not fully reflect official Russian policies, but behind both is arguably a vision of a unified information space under state jurisdiction which has clear, controlled, territorial borders.

This paper has demonstrated that, by using a novel approach applying delineation, protection, and control as analytical concepts to study national ideas about, and practical efforts to build, digital borders and digital sovereignty, it is possible to gain a comparative perspective of how geographic territory is projected into cyberspace through governmental control of specific elements of cyberspace. Digital borders could ensure the undisturbed functioning of this national segment which could be considered as a certain model for future 'digital border security', for example, a form of cyber security.

The building of digital borders and digital sovereignty must be seen as a collection of different technologies and policies. Because they are enacted on various levels and by different authorities, they are always multi-layered, complex, and conceptual issues. The analysis herein demonstrates that Russia is in the phase of delineating digital borders and progressing towards the phases of protection and control. This paper has provided a holistic view of the Russian efforts understood as a system-of-systems. The results of this analysis could also be used for determining if other states are engaged in the same process and what kind of similarities and differences these processes have. If international solutions to digital sovereignty are not found, these national segments of the Internet could make norms out of unilateral action. National segments of the Internet are becoming a reality, but the future Westphalian version of the Internet is still to be determined.

Currently, evaluating how the national segment of the Internet is developing in Russia and elsewhere is a constant necessity. In the future, some kind of methodology for monitoring the process of national segmentation of the Internet is needed. The authors suggest that one approach could be mapping and measuring Internet infrastructure. By measuring the level of infrastructure and protocols, researchers could collect comparative data on digital borders and use it to evaluate the technical level of digital sovereignty of an individual country or to make detailed comparisons between nations. Mapping the Internet infrastructure in a certain geographical space would allow researchers to study the rules of spatial arrangement of digital sovereignty and to estimate its infrastructural interrelationships, dependencies, development, and vulnerabilities. Consequently, researchers might be able to better evaluate the process of Internet segmentation.

References

Adler, R 2001, *Geographical Information in the Delimitation, Demarcation and Management of International Land Boundaries*, IBRU Boundary and Territory Briefing, vol. 3, no. 3, eds. Shelagh Furness & Clive H. Schofield, IBRU, Durham, UK, viewed 10 January 2018, <https://www.dur.ac.uk/ibru/publications/view/?id=219>.

Ashmanov, I 2013, *Doklad: Informatsionnyi suverenitet. Sovremennaia real'nost* (Presentation at iForum 24 April, Information sovereignty, contemporary reality), *Rossiia navsegda*, viewed 17 October 2016, <http://rossiyanavsegda.ru/read/948/>.

Bukharin, V 2016, *Komponenty tsifrovogo suvereniteta Rossiiskoi Federatsii kak tekhnitseskaia osnova informatsionnoi bezopasnosti* (Components of the digital sovereignty of the Russian Federation as technical basis of information security), *Vestnik MGIMO*, vol. 51, no. 6, pp. 76-90.

Choucri, N 2012, *Cyberpolitics in International Relations*, MIT Press, Cambridge, MA, US.

CSTO 2014, *Protokol o vzaimodeistvii gosydarstv - chlenov Organizatsii Dogovora o kollektivnoi bezopasnosti po protivodeistviiu prestupnoi deiatel'nosti v informatsionnoi sfere* (Interaction protocol of the member states of the organization of the collective security treaty on counteraction of criminal activity in information sphere), viewed 21 January 2018, <http://www.pravo.by/upload/docs/op/E71400003_1438290000.pdf>.

'delimitation' 2015, 'Glossary', *Introduction to Border Studies*, eds. S Sevastianov, J Laine & A Kireev, Dalnauka, Vladivostok, RU, pp. 388-97.

'demarcation 2015', 'Glossary', *Introduction to Border Studies*, Glossary, eds. S Sevastianov, J Laine & A Kireev, Dalnauka, Vladivostok, RU, pp. 388-97.

Demchak, C & Dombrowski, P 2013, 'Cyber Westphalia: Asserting state prerogatives in cyberspace', *The Georgetown Journal of International Affairs*, no. 20, pp. 29-38.

DeNardis, L 2014, *The global war for Internet governance*, Yale University Press, New Haven, CT, US.

Doktrina 2000, *Dokrina informatsionnoi bezopasnosti Rossiiskoi Federatsii* (Information security doctrine of the Russian Federation), 9 September, viewed 31 October 2016, <http://www.scrf.gov.ru/documents/6/5.html>.

Doktrina 2014, *Voennaia doktrina Rossiiskoi Federatsii* (Military Doctrine of the Russian Federation), 26 December 2014, viewed 20 January 2018, <http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf.>

Doktrina 2016, *Dokrina informatsionnoi bezopasnosti Rossiiskoi Federatsii* (Information security doctrine of the Russian Federation), 5 December, viewed 5 December 2016, <http://static.kremlin.ru/media/acts/files/0001201612060002.pdf>.

Dubov, D 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'*, vol. 4, no. 25, pp. 123-35.

Dylevskii, I, Komov, S, Korotkov, S, Rodionov, S & Fedorov, A 2007, *'Voennaia politika Rossiiskoi Federatsii v oblasti mezhdunarodnoi informatsionnoi bezopasnosti: regional'nyi aspekt'* (Military policy of the Russian Federation in the field of international information security: Regional aspect), *Voennaia mysl'*, no. 2, pp. 32-40.

Efremov, A 2016, *'Problemy realizatsii gosudarstvennogo suvereniteta v informatsionnoe sfere'* (Problems of realization of state sovereignty in the information space), *Vestnik UrFO*, vol. 2, no. 20, pp. 54-60.

——2017, *'Formirovanie kontseptsii informatsionnogo suvereniteta gosudarstva'* (Formation of the concept of state information sovereignty), *Pravo. Zhurnal vysshei shkoly ekonomiki*, no. 1, pp. 201-15.

Ermoshina, K & Musiani, F 2017, 'Migrating servers, elusive users: Reconfigurations of the Russian Internet', *Media and Communication*, vol. 5, no. 1, pp. 42-53.

Federal'nyi zakon 2017a, *O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii*, *no. 187-FZ*, (On the safety of the critical information infrastructure of Russian Federation), viewed 1 November 2017, <http://www.consultant.ru/document/cons_doc_LAW_220885/>.

——2017b, *O sviazi*, *no. 126-FZ (red. ot. 05.12.2017*) (On communications), viewed 11 January 2018, <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=284294&fld=134&dst=417,0&rnd=0.1557327116187115#0>.

——2017c, *Ob informatsii, informatsionnykh tekhnologiiakh i o zashchite informatsii*, *no. 149-FZ (red. ot. 25.11.2017)*, (On information, information technologies and information protection), viewed 21 January 2018, <http://www.consultant.ru/document/cons_doc_LAW_283382/>.

——2017d, *O gosudarstvennoi taine*, *no. 5485-1, (red. ot. 26.07.2017)*, (On state secret), viewed 21 January 2018, <http://www.consultant.ru/document/cons_doc_LAW_2481/>.

Freedom House 2017, *Freedom on the Net 2017: Russia,* viewed 11 January 2018, <https://freedomhouse.org/report/freedom-net/2017/russia>.

Federal Service for Technical and Export Control (FSTEK) 2016, *Svedeniia o polnomochiiakh FSTEK Rossii; perechen' normativnykh provovykh aktov, opredeliaiushchikh eti polnomochiia* (Information on the empowerment of FSTEC of Russia; A list of regulatory legal acts defining these empowerments), viewed 11 January 2018, <http://fstec.ru/obshchaya-informatsiya/polnomochiya>.

Golunov, I, Gorbachev, A & Turovskii, D 2017, *'Simona' v poiskakh mata i porno. 'Meduza' vyiasnila, kak rabotaiut sotrudniki Roskomnadzora, kotorye zanimaiutsia tsenzurnoi v CMI. I skol'ko eto stoit* ('Simona' in search for abusive language and porn. 'Meduza' found out how the employees of Roskomnadzor, who are engaged in censorship of the media, work. And how much it costs), *Meduza.io*, 8 December, viewed 20 July 2018, <https://meduza.io/feature/2017/12/08/simona-v-poiskah-mata-i-porno>.

International Telecommunication Union (ITU) 2015, *Global cybersecurity index & cyber wellness profiles April 2015*, viewed 23 January 2018, <http://handle.itu.int/11.1002/pub/80c63097-en>.

Kantyshev, P & Golits'na, A 2016, '*Runet budet polnost'iu obosoblen k 2020 godu*' (Runet will be completely isolated by 2020), *Vedomosti*, 13 May.

Kireev, A 2015, 'State border', *Introduction to border studies*, eds. S Sevastianov, J Laine & A Kireev, Dalnauka, Vladivostok, RU, pp. 98-117.

Kolomychenko, M & Makhukova, A 2017, '*Vne proslushki: pochemu Roskomnadzor i FSB sudiatsia s operatorami sviazi*', (Beyond wiretapping: Why Roskomnadzor and FSB are suing with telecommunication operators), *RBK: Ezhednevnaia delovaia gazeta,* 9 November.

Kontseptsiia 2013, *Kontseptsiia vneshnei politiki Rossiiskoi Federatsii*, *no. Pr-251* (Foreign policy concept of the Russian Federation), viewed 21 January 2018, <http://www.garant.ru/products/ipo/prime/doc/70218094/>.

Krygiel, A 1999, *Behind the wizard's curtain: An integration environment for a system of systems*, CCRP Publication Series, Institute for National Strategic Studies, Washington, DC, U.S.

Kudinov, V 2014, '*Formirovanie sistemy sovmestnoi okhrany gosudarstvennoi granitsy v svete realizatsii pogranitsnoi politiki Rossii*' (Formation of the system of joint protection of the state borders in the light of the implementation of the Russian border policy), *Problemy prava*, vol. 46, no. 3, pp. 110-15.

Kukkola, J 2018a, 'Civilian and military information infrastructure and the control of the Russian segment of Internet', Proceedings of *the 2018 International Conference on Military Communications and Information Systems (ICMCIS 2018)*, 22-23 May 2018, Warsaw, PL, pp. 1-8.

——2018b, 'New guidance for preparing Russian "digital sovereignty" released', *Finnish Defence Research Agency Research Bulletin 01 – 2018*, viewed 6 June 2018, <http://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+Tutkimuskatsaus+1-2018.pdf>.

——2018c. 'Russian cyber power and structural asymmetry', Proceedings of *the 13th International Conference on Cyber Warfare and Security (ICCWS)*, eds. J Chen & J Hurley, National Defense University, Washington, DC, US, 8-9 March, pp. 362-68.

Kukkola, J, Ristolainen, M & Nikkarila, J-P 2017, *Game changer: Structural transformation of cyberspace*, Finnish Defence Research Agency, Riihimäki, FI.

Libicki, M 2009, *Cyberdeterrence and cyberwar*, RAND, Santa Monica, CA, US.

Minkomsviaz 2017, "*O vnesenii izmenenii v Federal'nyi zakon "O sviazi" (Proekt)* (On the changes to the federal law, on communications, draft), 15 August, viewed 1 November 2017, <http://regulation.gov.ru/projects#npa=71277>.

Nocetti, J 2015, 'Contest and conquest: Russia and global Internet governance', *International Affairs*, vol. 91, no. 1, pp. 111-30.

Osnovy 2013, *Osnovy gosudarstvennoi politiki Rossiiskoi Federatsii v oblasti mezdunarodnoi informatsionnoi bezopasnosti na period do 2020 goda, No. Pr-1753* (Fundamentals of the state policy of the Russian Federation in the field of information security for the period up to 2020), viewed 21 January 2017, <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=178634&fld=134&dst=1000000001,0&rnd=0.520554609687278#0>.

Pan'shin, A 2017, *Glava 'Voentelekoma': tekhnologiia blokchein mozet poiavit'sia v armii Rossii* (Head of Voentelekom: Blockchain technology may appear in the Russian army), viewed 11 January 2018, <https://voentelecom.ru/news/novosti-kompanii/glava-voentelekoma-tekhnologiya-blokcheyn-mozhet-poyavitsya-v-armii-rossii/>.

Pilyugin, P 2017, '*Problemy opredeleniia granits v informatsionnom prostranstve*' (The problem of determining borders in the information space), *T-Comm: telekommunikatsiia i transport*, vol. 11, no. 8, pp. 37-44.

Plan 2018, *Plan meropriiatii po napravleniiu 'Informatsionnaia infrastruktura' programmy 'Tsifrovaia ekonomika Rossiiskoi Federatsii'* (Action plan in the direction of 'information infrastucture' of the 'digital economy of Russian Federation' program, appendix no. 3 to the minutes of the meeting 18 December 2017), viewed 11 January 2018, <http://www.consultant.ru/document/cons_doc_LAW_287865/>.

Polikarpov, V & Polikarpova, E 2014, '*Problema informatsionnogo suvereniteta Rossii*' (The problem of Russian information sovereignty), *Informatsionnoe protivodeitsvie ugrozam terrorizma*, no. 23, pp. 285-90.

Polozhenie 2016 *Polozhenie o Federal'noi sluz'be po nadzory v sfere sviazi, informatsionnykh tekhnologii i massovykh kommunikatsii 16.03.2009, no. 228 (red. ot 01.07.2016)* (Regulations of the Federal service for supervision of connections, information technology and mass communications March 16, 2009, no. 228, updated July 1, 2016), viewed 11 January 2018, <https://rkn.gov.ru/about/p179/>.

Postanovlenie 2018, *Ob utverzhdenii Pravil kategorirovaniia ob''ektov kriticheckoi informatsionnoi infrastuktury Rossiiskoi Federatsii, no. 127* (About the approval of the rules of categorization of the objects of critical information infrastructure of the Russian Federation, no 127), 8 February 2018, viewed 6 June 2018, <http://www.consultant.ru/document/cons_doc_LAW_290595/>.

Prikaz 2016a, *Prikaz Federal'noi slyzby okhraniy Rossiiskoi Federatsii ot 07.09.2016, no. 443: Ob utberzdenii Polozeniia o rossiiskom gosudarstvennom segmente informatsionno-telekommunikatsionnoi seti 'Internet'* (Order of the Federal security service of the Russian Federation from September 7, 2016, no. 443: On the approval of the regulations of the Russian state segment of the information-telecommunication network 'Internet'), viewed 10 January 2018, <http://publication.pravo.gov.ru/Document/View/0001201610170008?index=0&rangeSize=1>.

——2016b, *Prikaz no. 41821, 23 marta 2016 goda* (Order no. 41821, March 23, 2016), viewed 11 January 2018, <http://www.fsb.ru/files/PDF/prikaz_182.pdf>.

Programma 2014, *Gosudarstvennaia programma Rossiiskoi Federatsii "Informatsionnoe obshchectvo (2011-2020 gody)", no. 313* (The Russian Federation state project: "Information society [2011-2020], no. 313)", viewed 21 January 2018, <http://www.consultant.ru/document/cons_doc_LAW_162184/>.

Programma 2017, *Tsifrovaia ekonomika Rossiiskoi Federatsii, no. P-1632-p* (State project: Digital economy of Russian Federation, no. R-1632-r), viewed 23 January 2018, <http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf>.

Ristolainen, M 2017, 'Should "RuNet 2020"' be taken seriously? Contradictory views about cybersecurity between Russia and the West', *Journal of Information Warfare*, vol. 16, no. 4, pp. 113-31.

Roskomsvoboda 2017, *'Kitaizatsiia' Runeta vkhodit v aktivnuiu fazu i nachetsia s tochek obmena trafikom* (The 'Sinofication' of the Russian Internet enters its active phase and it will start on the traffic exchange points), viewed 21 January 2018, <https://roskomsvoboda.org/31224/>.

——2018, *Rostelekom gotov ychastvovat' v razrabotke rossiiskogo kocmicheskogo interneta* (Rostelecom is ready to participate in the development of the Russian space Internet), viewed 21 January 2018, <https://roskomsvoboda.org/39171/>.

Rostelekom 2018a, *Magistral'naia set' sviazi* (Backbone network), viewed 21 January 2018, <https://www.rostelecom.ru/about/net/magistr/>.

——2018b, *Universal'nye uslugi sviazi i proekt ustarennia tsifrovogo neravnstva* (Universal connection services and a project to eliminate digital inequality), viewed 10 January 2018, <https://www.rostelecom.ru/projects/uus/>.

Rossiiskii soiuz promyshlennikov i predprinimatelei (RSPP) 2017, *Komissiia po sviazi i informatsionno-kommunikatsionnym tekhnologiiam - otchet o rabote Komissii v 2017 gody* (Commission on connections and information and communication technologies – Report of the work of the Commission in 2017), viewed 21 January 2018, <http://media.rspp.ru/document/1/9/2/9253e2f15a4b9c055bd0b9b1a271ed0a.docx>.

Security Council of the Russian Federation (SCRF) 2017, *Vypiska iz Osnovnykh napravlenii nauchnykh issledovanii v oblasti obespecheniia informatsionnoi bezopasnosti Rossiiskoi Federatsii* (Extract from the Main directions of scientific research in the field of information security of the Russian Federation), viewed 21 January 2018, <http://www.scrf.gov.ru/security/information/document155/>. & Kireev A 2015, *Introduction to Border Studies*, Danuika, Vladivostok, RU.

Sheldon, J 2013, 'The rise of cyberpower', *Strategy in the contemporary world: An introduction to strategic studies*, eds. J Baylis, J Wirtz & C Gray, Oxford University Press, Oxford, UK, pp. 282-98.

Soldatov, A 2017, 'The taming of the Internet', *Russian Social Science Review*, vol. 58, no. 1, pp. 39-59.

Strategiia 2009, *O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii do 2020 goda* (On the national security strategy of the Russian Federation until 2020), viewed 27 September 2017, <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102129631>.

Strategiia 2017, '*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), viewed 24 July 2017, <http://static.kremlin.ru/media/acts/files/0001201705100002.pdf>.

Streltsov, A & Pilyugin, P 2016, '*K voprosu o tsifrovom suverenitete*' (About digital sovereignty), *Informatizatsiia i sviaz'*, no. 2, pp. 25-30.

Sukharevskaia, A & Iuzbekova, I 2016, *Lishnego ne utechet: Kak imenno chinoviki namereny obezopasit' Runet* (Unnecessary will not leak: How the officials intend to protect Runet), *RBK: Ezhednevnaia delovaia gazeta*, 17 June.

Tikk, E 2017, 'International cyber norms dialogue as an exercise of normative power', *Georgetown Journal of International Affairs*, vol. 17, no. 3, pp. 47-59.

Tsarenkova, N 2016, '*Pogranichnye organy FSB Rossii v sisteme obespecheniia natsional'nykh interesov Rossiiskoi Federatsii v pogranitsnom sfere*' (Border authorities of FSB in the system of ensuring national interests of the Russian Federation in the border sphere), *Nauchno-prakticheskii zhurnal "Gosudarstvo i pravo v XXI veke",* no. 1, pp. 52-8.

Tuukkanen, T 2013, 'Sovereignty in the cyber domain', *The fog of cyber defence*, eds. J Rantapelkonen & M Salminen, National Defence University, Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection 10, Helsinki, FI, pp. 37-45.

Ukaz 2015, *Ukaz prezidenta RF O nekotorykh voprosakh informatsionnoi bezopasnosti Rossiiskoi Federatsii, no. 260* (Presidental order on some issues of the information security of the Russian Federation, no. 260), viewed 11 January 2018, <http://publication.pravo.gov.ru/Document/View/0001201505220028 >.

United Nations 2011, *Letter dated 12 September 2011 from the Permanent and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359)*, viewed 21 January 2018, <http://undocs.org/A/66/359>.

——2015, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/69/723)*, viewed 21 January 2018, <http://undocs.org/A/69/723>.

Yin, R 2009, *Case study research: design and methods*, 4th ed., SAGE Publications, London, UK.

Zukova, K 2017, *GosSOPKA sdadut pod kliuch - Solar Security i Positive Technologies zaimutsia sozdaniem tsentrov kiberbezopasnosti* (GosSOPKA will hand over turnkey - Solar Security and Positive Technologies will create cyber security centers), *Kommersant*, 20 November.

New Guidance for Preparing Russian 'Digital Sovereignty' Released

Juha Kukkola

Abstract

This paper analyses the latest developments of the Russian project to build 'digital sovereignty'. More precisely it examines how the Program of Digital economy of Russian Federation (*Tsifrovaia ekonomika Rossiiskoi Federatsii*)[1][2] is being planned to be implemented in the light of the action plans approved in January – February 2018.[3] This paper focuses on 'directions' (*napravlenie*) of 'information security' (*informatsionnaia bezopasnost'*) and 'information infrastructure' (*informatsionnaia infrastructura*) of the 'Digital economy'. Furthermore, 'directions' are approached through the concepts of shaping of cyberspace, controlling the national segment of the Internet, and digital sovereignty.[4] These concepts connect the 'Digital economy' and its 'directions' to the project started by the Russian government in 2014 to create a self-sustained national Internet.[5] This paper stresses that Russian

[1] Note on transliteration and translation: Russian words are transliterated according to the Library of Congress system. The titles of documents and specific noteworthy concepts are given in translated form with transliterations.

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

[3] The Government of the Russian Federation. *O "dorzhnykh kartakh" po napravleniiam programmy "Tsifrovaia ekonomika Rossiiskoi Federatsii"* Official webpage, 9 February 2018 [Online]. Available: http://government.ru/orders/selection/401/30895/ [Accessed 22 March 2018].

[4] Shaping of cyberspace is understood as state efforts to influence the structure of cyberspace by technological, administrative and political means to gain, for example, military advantage. Controlling of the national segment of the Internet is understood as projecting state power and authority to cyberspace through information infrastructure located in its territory. Digital sovereignty is understood as projecting state sovereignty to cyberspace. It is the ultimate objective of controlling the national segment of the Internet.

[5] Golitsyna, Anastasiia, Ser'gina, Elizaveta and Kozlov, Petr. "Gosydarstvo khochet kontrolirovat' marshruty internet-trafika v strane." *Vedomosti*, 11 February 2016 [Online]. Available: https://www.vedomosti.ru/politics/articles/2016/02/11/628508-gosudarstvo-hochet-kontrolirovat-rossiiskii-zarubezhnii-internet-trafik-strane [Accessed 24 March 2018].

'digital' socio-economic plans have also a military strategic character.

The first version of this paper was published by Finnish Defence Research Agency as Research Bulletin 01 – 2018 (April 10, 2018).

1 Strategic Planning and Digital Economy

The Digital economy of the Russian Federation (*Tsifrovaia ekonomika Rossiiskoi Federatsii*)[6] is a government program based on the Strategy of the development of information society in Russian Federation in 2017-2030 (*Strategii razvitiia informatsionnogo obshchestvo v Rossiiskoi Federatsii na 2017-2030 gody*)[7] and, to a lesser extent, Information Security Doctrine of Russian Federation (*Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii*)[8].[9] They are both part of the strategic planning process of the state defined in the Law on Strategic planning (*O strategicheskom planirovanii v Rossiiskoi Federatsii*).[10] The strategic planning consists of goal-setting, forecasting, planning, and developing programs for social-economic progress and national security of the Russian Federation and its subjects. In the context of strategic planning, all the above-mentioned documents have both socio-economic and (military) security aspects. For example, the Strategy of the development of information society declares, in addition to socio-economic issues, as its

---

[6] The Government of the Russia Federation, Programma "Tsifrovaia ekonomika Rossiiskoi Federatsii."

[7] The President of the Russia Federation. *Ukaz "O strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2030 gody" No. 203* 9 May 2017 [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf [Accessed 22 September 2017].

[8] The President of the Russian Federation. *Ukaz "Dokrina informatsionnoi bezopasnosti Rossiiskoi Federatsii" No. 646* 5 December 2016 [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf [Accessed: 12 September 2017].

[9] Another important document is the Strategy of Scientific-Technological Development of the Russian Federation (The President of the Russian Federation. *Ukaz "O Strategii nauchno-tekhnologicheskogo razvitiia Rossiiskoi Federatsii" No. 642* 1 December 2016 [Online]. Available: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=207967&fld=134&dst=1000000001,0&rnd=0.03632307878975349#027545814856013906 [Accessed: 22 March 2018].)

[10] Federal'nyi zakon. *"O strategicheskom planirovanii v Rossiiskoi Federatsii" N. 172-F3* 28 June 2014 (amended 31.12.2017) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_164841/ [Accessed: 22 March 2018].

objectives the protection of critical information infrastructure and the securing of the unity of communication networks for defence purposes.[11] Similarly, Information Security Doctrine combines strategic deterrence and prevention of conflicts arising from the use of information technology with innovation and economic competitiveness.[12]

The Program of Digital Economy takes its guidance from the Strategy and Doctrine and sets its objectives and tasks in the context of five directions (*napravlenie*): normative regulation, cadres and education, research and technical reserves, information infrastructure and information security. The last two are of interest when examining how Russia is shaping cyberspace and trying to achieve 'digital sovereignty'. In the Program, information infrastructure is intertwined with information security. Objectives and tasks are based on external and internal challenges and threats (the emphasis is clearly on adversary state actors) the main objective being: "ensuring the unity, stability and security of information-telecommunication infrastructure of the Russian Federation on all levels of information space".[13] Like the previously mentioned Strategy and Doctrine, the Program also combines security with economy by emphasising the use of domestic software, hardware, and cryptographic solutions. Most interestingly, the Program presents a 'road-map' which states that in 2020 Russia will ensure its 'digital sovereignty' (*tsifrovoi suverenitet*) and by 2024 it will be one of the leading states in information security. In connection with this, according to the Program in 2024 only 10% of internal traffic of the 'Russian segment of the Internet' (*Rossiiskii segment seti "Internet"*) will be routed through foreign servers.[14]

In December 2017 the 'Government commission on the use of information technology to improve the quality of life and business conditions' (*Pravitel'stvennaia komissiia po ispol'zovaniiu informatsionnykh tekhnologii dlia uluchsheniia zhizni i uslovii vedeniia predprinimatel'skoi deiatel'nosti*) approved actions plan for four of the five 'directions' of

---

[11] The President of the Russian Federation, "*O strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2030 gody*."
[12] The President of the Russian Federation, "*Dokrina informatsionnoi bezopasnosti Rossiiskoi Federatsii*."
[13] The Government of the Russian Federation, Programma "Tsifrovaia ekonomika Rossiiskoi Federatsii".
[14] Ibid. For the background of this project cf. Ristolainen, Mari. "Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security Between Russia and the West," *Journal of Information Warfare*, vol. 16, no. 4, pp. 113-131, 2017.

Program of the Digital economy.[15] The fifth, cadres and education, was approved in February 2018.[16] According to the action plans the total budget of the 'Digital Economy' will be 522 billion roubles (8,9$ bn) for the period 2018-2020.[17] The responsibility for implementing the 'directions' of 'information infrastructure' and 'information security' was given to Minkomsviaz' (Ministry of Telecom and Mass Communications of the Russian Federation) and a non-commercial organisation 'Digital Economy' (*ANO Tsifrovaja Ekonomika*) was created to coordinate public and private activities and to monitor the realization of the state program.[18] Currently, the 'Digital Economy' organization includes representatives from the Russian government and all the leading Russian IT-firms.[19] It should be noted that the official presence of security and military institutions in this organization is light.

2 Information Infrastructure

Practically all state security ministries and agencies are listed as responsible actors for 'the direction of Information infrastructure'.[20] The same applies

---

[15] The Government of the Russian Federation. *O "dorzhnykh kartakh" po napravleniiam programmy "Tsifrovaia ekonomika Rossiiskoi Federatsii."* Official webpage, 9. February 2018 [Online]. Available: http://government.ru/orders/selection/401/30895/ [Accessed: 22 March 2018].

[16] The Government of the Russian Federation. *Utverzhen plan meropriiatii po napravleniiu "Kadry i obrazovanie" programmy "Tsifrovaia ekonomika Rossiiskoi Federatsii."* Official webpage, 21 February 2018 [Online]. Available: http://government.ru/news/31428/ [Accessed: 22 March 2018].

[17] Only aprox. 130 billion roubles (2,2$ bn) will be funded from the federal budget. Federal spending was 3974 billion roubles in 2017. (Tishina, Iuliia and Zukova, Kristina. Otsifrovannye milliardy - Pravitel'stvo utverdilo proekty "Tsifrovoi ekonomiki." *Kommersant*, 10 January 2018 [Online]. Available: https://www.kommersant.ru/doc/3515334 [Accessed: 22 May 2018]; Trading Economics. Russian government spending. Webpage, 9 April 2018 [Online]. Available: https://tradingeconomics.com/Russia/government-spending [Accessed: 9 April 2018].)

[18] The Government of the Russian Federation. *Postanovlenie "O sisteme upravleniia realizatsiei programmy "Tsifrovaia ekonomika Rossiiskoi Federatsii"" No. 1030* 28 August 2017 [Online]. Available: http://static.government.ru/media/files/zutOPH6TyKz2ciJAFcn74orvpb89UCMa.pdf [Accessed: 22 May 2018].

[19] Tsifrovaia ekonomika. "*Tsifrovaia ekonomika*." Official webpage, 22 March 2018 [Online]. Available: https://data-economy.ru/ [Accessed: 22 March 2018].

[20] Federal Security Service (FSB), Federal Protective Services (FSO), Ministry of Interior (MVD) and Ministry of Defence (MOD) are mentioned. Also listed are Federal Service for Technical and Export Control (FSTEK) and The Federal Service for Supervision of Communications, Information Technology and Mass Media (Rozkomnadzor) and Rossviaz' (Federal Communications Agency). The main partners

to major IT-companies which are listed as participating contractors. The main objectives of 'the direction' are: Sufficient communication network; domestic infrastructure for data storage and processing which provides affordable, sustainable, safe, and cost-effective services; and sufficient digital platforms for the needs of citizens, business and the government.
In practice, the first objective includes, for example, creating a normative base for the use of information technology[21], high-speed Internet (100Mb/s) to almost every household and government institution by 2024[22], speech and data connection to all priority objects of transport infrastructure[23], the implementation of 5G technology by the economy[24], developing state-wide narrow-band IoT network (LPWAN), and state wide (including EEZ) satellite services[25]. The second objective includes, for example, the establishment of federal data-centres (eight by 2024)[26] and unified cloud services for the government. The third objective includes, for

---

are Skolkovo foundation, M. V. Lomonosov Moscow university, Higher School of Economics, all the major IT-firms and the Central Research Institute of Communications (FGUP TsNIIS) (which is responsible for the development of SORM) (Government commission. "*Plan meropriiatii po napravleniiu "Informatsionnaia infrastruktura" programmy "Tsifrovaia ekonomika Rossiiskoi Federatsii".*" Appendix N. 3 to the minutes of the meeting 18 December 2017 [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_287865/ [Accessed: 22 March 2018]; TsNIIS. "SORM" Official webpage, 22 May 2018 [Online]. Available: https://zniis.ru/focus/sorm [Accessed: 22 March 2018].)

[21] The participation of the Ministry of Defence in this project implies the use of Wi-Fi and other radio frequency based technologies to create backbone connections and the need to coordinate the use of electro-magnetic spectrum.

[22] Rostelekom is designated as the main provider. FSO is responsible for the networks of federal organizations and supervises their connections.

[23] This consists of, for example, highways and railroad lines.

[24] This includes Russian software, encryption, and SIM cards. FSB, FSO and MOD have a significant role in this task. Technology is based on 5G/IMT-2020 with SDN/NFV virtualization, Cloud RAN and Virtualized backhaul. Planned frequencies are: 694-790 MHz; 3,4-3,8 GHz; 4,4-4,99 GHz, 5,9 GHz, 24,25-29,5 GHz, 30-55 GHz, 66-76 GHz, 81-86 GHz.

[25] This includes 'GIMSS' 'Global multifunctional info-communication satellite system' (*Global'noi mnogofunktsional'noi infokommunikatsionnoi sputnikovoi sistemy*) which might be a LEO satellite system analogous to OneWeb (Balashova, Anna, Sidorkova, Inna and Kolomychenko, Mariia. "Pravitel'ctvu predlozat sozdat' global'nuiu set' za R299 mlrd." *RBC*, 22. November 2017 [Online]. Available: https://www.rbc.ru/technology_and_media/22/11/2017/5a159bdb9a79476a55456d2b?from=center [Accessed: 22 March 2018]). LPWAN means Low-Power Wide-Area Network and EEZ Exclusive Economic Zone.

[26] Situated in Central (*Tsentral'nii*), North-Western (*Severo-Zapadnii*), Uralskii (*Ural'skii*), Siberian (Sibirskii), Privolzhzkii (*Privolzhkii*) and Far-Eastern (*Dal'nevostochni*i) federal districts (*federal'nyi okrug*) and probably in two more to ensure resiliency of the system.

example, e-government services and their management systems, space based remote sensing system and geodetic control network, and services based on these systems. 'The direction of information infrastructure' is the most expensive one and amounts to circa 436 billion roubles (7,6$ bn). FSB, FSO and FSTEK have a definite role in planning these projects but implementation is left to state corporations and the private sector.

3 Information Security

'The direction of information security' does not, somewhat surprisingly, include the Ministry of Defence in its list of responsible actors, although, it is consulted in some of the projects.[27] All the other security ministries and agencies are present.[28] The main objectives of information security are: Ensuring the unity, stability and security of the information-telecommunication infrastructure of the Russian Federation on all levels of information space (*informatsionnoe prostranstvo*)[29]; ensuring organizational and legal protection of the individual, business and state interests in the framework of the digital economy; and the creation of conditions for Russia's leading position in the export of information security services and technologies; as well as the integration of national interests in the international documents on information security issues.

The first objective is defined by its indicators to mean decreasing the percentage of routing domestic traffic through foreign servers to 10% by 2024, the almost total replacement of foreign produced hardware and software by domestic versions in federal and local administrative organizations, state corporations and corporations connected to the state, and the comprehensive implementation of Russian standards of information security by those same actors by 2024. In practice, the stability and security (*ustoichivost' and bezopasnost'*) of 'the unified telecommunications network of the RF' is guaranteed, firstly, by defining

---

[27] Government commission. "*Plan meropriiatii po napravleniiu "Informatsionnia bezopasnost'" programmy "Tsifrovaia ekonomika Rossiiskoi Federatsii"*." Appendix N. 4 to the minutes of the meeting 18 December 2017 [Online]. Available: http://static.government.ru/media/files/AEO92iUpNPX7Aaonq34q6BxpAHCY2umQ.pdf [Accessed: 22 March 2018].

[28] The main partners include, for example, the Cryptographic academy of the Russian Federation and a group of lesser known corporations and institutions.

[29] "A set of information resources created by the subjects of the information sphere, the means of interaction of such subjects, their information systems and the necessary information infrastructure" (The President of Russian Federation. "*O strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2030 gody*.")

the vulnerabilities of networks.[30] Based on the analysis and normative work, a 'centralized system of monitoring and managing the public communication networks' is to be established. This is an organizational and technological project, which is managed by a designated operator, and includes the Ministry of Defence. It functions in cooperation with National coordination centre of computer incidents (NKTsKI).[31] The system should be up and running by 2020. Stability and security includes also the creation of standards for domestic cloud, fog computing, and quantum technology, and for systems of augmented reality and artificial intelligence.

The manageability and reliability (*upravliaemost' and nadezhnost'*) aspect of the first objective concentrates on the 'Russian segment of the Internet' and 'circuiting' (*zamykanie*)[32] its network traffic exclusively inside the territory of the Russian Federation. The software component of this project consists of the following subsystems: register of routing-address information (Internet Number Registry), monitoring of routing information (Internet Routing Registry), nationally controlled DNS root-servers, blocking of unlawful content, cooperation with NKTsKI, and national certificate authority centre.[33] The subsystems should be managed by a designated operator. Furthermore, the technological independence and security of data processing infrastructure and systems should be guaranteed. This is connected to import-substitution and domestic

[30] This includes stability of public communication networks, vulnerability of mobile networks (SS7 and Diameter protocols), vulnerability of transit traffic, vulnerabilities arising from the use of foreign technology, and vulnerabilities caused by cybercrime.

[31] This is a suborganization of the FSB designated to manage GosSOPKA [see footnote 35] and to coordinate actions involving critical information infrastructure (The president of the Russian Federation. *Ukaz "O sovershenstvovanii gosudarstvennoi sistemy obnaruzheniia, preduprezheniia i likvidatsii posledstvii komp'iuternykh atak na informatsionnye resursy Rossiiskoi Federatsii" No.620* 22 December 2017 [Online]. Available: http://kremlin.ru/acts/bank/42623 [Accessed: 22 May 2018]; FSB. Law project "*O Natsional'nom koordinatsionnom tsentre po komp'iuternym intsidentam*" (prepared by FSB 26.12.2017) 23 January 2018 [Online]. Available: https://www.garant.ru/products/ipo/prime/doc/56640460/ [Accessed: 22 March 2018].) Interestingly, FSTEK, which is under the MOD, is the federal agency responsible for the security of critical information infrastructure (The President of the Russian Federation. *Ukaz "Vobrosy Federal'noi sluzhby po tekhnicheskomu i eksportnomu kontroliu" No. 1085* 16 August 2004 (amended 25.11.2017) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_14031/ [Accessed: 22 March 2018].)

[32] This term seems to refer to Internet backbone architecture based on circuit switching. The document does not specify what OSI layer level is being discussed.

[33] Cf. Roskomsvoboda. *"Kitaizatsiia" Runeta vkhodit v aktivnuiu fasu i nachnetsia s tochek obmena trafikom*. Webpage, 18 August 2017 [Online] Available: https://roskomsvoboda.org/31224/ [Accessed: 24 March 2018].

production of hardware and software. Objectives are achieved, on the one hand, by encouraging innovation and government projects and, on the other hand, by regulation.

Security in the context of the 'Digital economy' is not only understood as 'cybersecurity'[34] but also in the context of national interests, among others national defence. Security is not only a technological issue but also a normative one: Cloud service provider's use of data should be regulated, security standards for big data (*bol'shie dannye*) management should be enforced, the criminal code should be updated, and users of communication networks should be identified. The significance of the last, quite minimally described, task should not be under estimated. It is 'hidden' among the tasks defining the rules for managing personal data. Identification of users would, in practice, erase anonymity from RuNet. Interestingly, there is also a plan to enforce domestic anti-virus software on all personal computers in Russia. The 'Digital economy's' security concept also reflects Russian understanding of information threats by including prevention of the dissemination of 'unlawful information' (*protivopravnaia informatsiia*).

In this context, security seems to be connected to multiple different systems of information sharing between officials and private citizens, and to the filtering of traffic. Such a system of systems should provide indicators of harmful activity to National and Regional Computer Incident Response Centres (NKTsKI and RKTsKI). Although this is not stated directly, the arrangement seems to refer to GosSOPKA[35] system. It could also refer to

---

[34] The project mentions domestic biometric authentication, multifactor authentication, digital identification, cryptographic authentication, trusted third party authentication, TLS with Russian crypto algorithms; and, also, operating systems, database management systems, and office software (i.e. national application family i.e. 'The Resource').

[35] The GosSOPKA (*Dosudartsvennia Sistema obnaruzheniia, preduprezdeniia i likvidatsii posledsvii komp'iuternykh atak*) is "[…] a single territorially distributed complex, including forces and means designated to detect, prevent and eliminate the consequences of computer attacks and respond to computer incidents" (Federal'nyi zakon. "O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii" No. 187-F3 26 July 2017 [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_220885/ [Accessed: 1 November 2017].) The project of building GosSOPKA was initiated in 2013 by president Vladimir Putin (The President of the Russian Federation. "Vypiska iz kontseptsii gosydarstvennoi sistemy obnaryzeniia, preduprezdeniia i likvidatsii posledstvii komp'iuternykh atak na informatsionnye resursy Rossiiskoi Federatsii" No. 1274 12 December 2014 [Online]. Available: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=181661&fld=134&dst=1000000001,0&rnd=0.556811797145774#046144179472131297 [Accessed: 24 March 2018].). It has been envisioned as a centrally controlled national SIEM (Security

'the centralized system of monitoring and managing the public communication networks' which was mentioned in 'the information infrastructure direction.' In any case, both are managed by FSB.

The third objective of information security is connected to the creation of export markets for Russian IT-solutions but also includes wider foreign policy goals. This becomes clear when the term 'cyberphysical' (*kiberfizicheskii*) system is introduced and it is connected to IoT (Internet of Things) and to critical information infrastructure. The term's definition is left open, but it is preliminarily put into a legal-normative framework where unauthorized interference of 'cyberphysical' systems should be proscribed. This new term has a clear connection to the previous Russian endeavour in the United Nations to ban cyber weapons.[36]

The foreign policy character is emphasized in how Russian information security standards should be harmonized with international ones, but only with the participation of Russian experts in defining international ones and keeping them in line with Russian interests. This includes the promotion of Russian, mainly cryptographic, solutions abroad. One of the main spheres of action in this regard is Eurasian Economic Union.[37] Finally, 'the Concept of secure functioning and development of the Internet' is to be prepared and presented to international organizations (it may include multiple sub-concepts and normative initiatives). This policy initiative includes provisions on: Information, technological, and economic state sovereignty in national segments of the Internet; confidentiality of data and security of users[38]; and equal participation of members of world community to the governance of global information network. This project should be

---

Information and Event Management system) (Solar Security. "*Reshenie po cozdaniiu tsentrov GosSOPKA ot Solar JSOC*." Official Webpage. https://solarsecurity.ru/upload/pdf/Solar_JSOC_GOSSOPKA.pdf [Accessed: 24 March 2018].

[36] Kavanagh, Camino. *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*. UNIDIR 2017 [Online] Available: http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf [Accessed 24 March 2018].

[37] In this context common normative regulation and standards, joint exercises, and 'a zone of digital trust' (including the use of blockchain technology) are mentioned.

[38] The document explicitly states that confidentiality and security categorically exclude anonymity of users, irresponsibility of users and 'the impunity of offenders' (*beznakazannost' pravonarushitelei*). This definition follows the observed Russian state policy to restrict privacy in Internet. (Freedom house. *Freedom on the Net 2017 – Russia*. 2017 [Online]. Available: https://freedomhouse.org/report/freedom-net/2017/Russia [Accessed: 9 April 2018].)

completed, in accordance with Russian interests, by the end of 2020. All the objectives of information security should be achieved with 34 billion roubles (600$ million).

4 Self-Sustained National Internet by 2024?

The 'Digital economy' program might seem overly ambitious. Then again, Rostelekom and other IT-companies have already produced impressive results in building up Russia's IT-infrastructure and the state has invested significantly in domestic hardware and software production.[39] Rostelekom has also gained control of many of the subsystems mentioned in the documents.[40] Additionally, FSB and FSTEK already have the normative base for taking control of Russia's critical information infrastructure.[41] Furthermore, the Russian state is openly challenging the freedom and openness of the Russian Internet – and winning.[42] And, after the fall of UN GGE process[43], Russia is preparing to push its normative view of state sovereignty in cyberspace through different venues.[44]

---

[39] The Federal Agency for Press and Mass Communications. *Internet v Rossii 2016 gody: Sostoianie, tendentsii i perspektivy razvitiia*. Москва, 2017 [Online]. Available: http://www.fapmc.ru/rospechat/activities/reports/2017/teleradio/main/custom/00/01/file.pdf [Accessed: 24 March 2018].; RAEK. *Ekonomika RuNeta 2017*. [Online] Available: http://raec.ru/upload/files/de-itogi_booklet.pdf [Accessed: n24 March 2018].; Minkomsviaz'. *Godovoi otchet o khode effektivnosti gosydarstvennoi programmy Rossiiskoi Federatsii "Inoformatsionnoe obchshestvo (2011-2020 gody)*" 25 April 2017 [Online]. Available: http://minsvyaz.ru/uploaded/files/otchet2016.pdf [Accessed: 24 March 2018].

[40] Balashova, Anna and Kanev, Petr. "Rostelekom" stal operatorom reestra domenov .ru i .рф. *RBC*, 23 January 2018 [Online]. Available: https://www.rbc.ru/technology_and_media/23/01/2018/5a675ab29a79473a982cd704 [Accessed: 24 March 2018].

[41] The President of the Russian Federation, "Dokrina informatsionnoi bezopasnosti Rossiiskoi Federatsii."

[42] Li, Irina. Bez Telegram: 4 voprosa o vozmozhnoi blokirovke messendzhera v Rossii. *RBC*, 21 March 2018 [Online]. Available: Россииhttps://www.rbc.ru/technology_and_media/20/03/2018/5ab0f8439a794710eb5972ac?from=center_5 [Accessed: 24 March 2018].

[43] UN Group of Governmental Experts on Developments in the field of Information and Telecommunications in the Context of International Security. For more about this process cf. Tikk, Eneken and Kerttunen, Mika. *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*. Cyber Policy Institute, 2017 [Online]. Available: cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf [Accessed: 9 April 2018].

[44] The Russian ministry of foreign affairs. *Vystuplenie Zamestitelia Sekretaria Soveta Bezopasnosti Rossiiskoi Federatsii O.V. Khramova na mezhdunarodnoi konferentsii OBSE po kiberbezopasnosti, g..Vena, 3 noiabria 2017 goda.* Official webpage 3

The ‘Digital economy’ brings together policies and projects which have already been in progress for some time. Moreover, although the program relies heavily on extra-budgetary funds and is financially quite modest – the planned budget for the state armament program for 2018-2027 is 300$ mrd[45] – many of its objectives can be achieved through legislation, reorganization and reallocation of resources. This could mean that some parts of ‘Digital sovereignty’ are achieved quite rapidly and effortlessly. Of course, Western sanctions and the development of the global economy might have adverse effects on the program. It is also important to note that ‘the directions’ of ‘Digital economy’ have planned funding only to 2020. There are many economic and political variables, including the development of international relations and the Russian presidential elections in 2024, which could affect the realization of a self-sustained national Internet by 2024.

5 Discussion

The program of Digital economy is much more than a plan to push Russia into the information age. It is both an economic and a national security project. It aims to shape cyberspace by creating a self-sufficient and territorially based island of the Internet where Russian state sovereignty is normatively and technologically undisputed. This subspace is based on domestically produced software and hardware infrastructure. It is controlled centrally by security services and its content and processes are subjugated to the interests of the authoritarian state – in the name of security. Controlling the national segment of the Internet means government control over traffic, services, and users.

There is no doubt that the ‘Digital economy’ is a foundation for digital sovereignty. It is openly stated in the documents discussed in this paper. This sovereignty is based on censorship, monitoring, filtering, controlling, and domestic production and ownership of the information infrastructure. In the best case for Russia, economic benefits will flow from this project and Russia will be able to sell its version of the Internet (and domestically produced technology with it) to its allies. If this fails, Russia will ensure

November 2017 [Online]. Available: http://www.mid.ru/web/guest/foreign_policy/rso/osce/-/asset_publisher/bzhxR3zkq2H5/content/id/2938933 [Accessed: 24 March 2018].

[45] Bocharova, Svetlana and Nikol’ckii, Aleksei. Putin soobchshil o priniatii novoi gosprogrammy vooryzhenii. *Vedomosti*, 24 January 2018 [Online]. Available: https://www.vedomosti.ru/economics/articles/2018/01/24/748864-putin-vooruzhenii [Accessed: 9 April 2018].

national cyber defence and resiliency of its networks based on the disconnection of its national segment from the global Internet and will achieve authoritarian control of its (cyber) civil society.

Still, the worst case would be for Russia to remain an outlier of the global cyber community – as a pariah state relying on domestic, subpar solutions with an inefficient IT-sector. The 'Digital economy' is reminiscent of Soviet style five-year plans or a more recent state armament program. Neither of these produced 100% of the objectives sought. The creation of an information society based on a vertically controlled government program will have its pitfalls. Be that as it may, it should be kept in mind, that the military strategic part of the 'Digital economy' (security) will cost only 1/10 of the creation of an information society (infrastructure). This, when all is said and done, is 'a military strategic idea that promises a cost-effective solution for strategic deterrence against perceived threats'.[46]

[46] Kukkola, Juha, Ristolainen, Mari & Nikkarila, Juha-Pekka. *Game Changer. Structural transformation of cyberspace*. Riihimäki: Finnish Defence Research Agency, 2017 [Online]. Available: http://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+julkaisuja+10.pdf/5d341704-816e-47be-b36d-cb1a0ccae398 [Accessed: 9 April 2018]. ISBN 978-951-25-2954-4.

Modelling Closed National Networks - Effects in Cyber Operation Capabilities

Juha-Pekka Nikkarila
Bernt Åkesson
Vesa Kuikka
Juhani Hämäläinen

Abstract

We introduce a mathematical model to describe how operational capabilities are affected when a nation closes their national networks. When considering defensive capabilities, we define capability as a probability for denying adversarial operations in a friendly network so that the overall system (Cf. critical infrastructure) remains operative. We define an operation as a set of actions that are conducted against one specific subsystem. The overall system is considered to be operative when at least predefined number (M) of subsystems is operative. The probability of having exactly k operative subsystems out of N is given by the probability mass function of the Poisson binomial distribution. The probability of subsystem i being operative depends on whether it is under attack or not. Under normal conditions, the subsystem is operative with a certain probability. When the subsystem is under attack, the probability of a successful computer network defense operation of the subsystem is described as a probability for denying the operation in at least one of its steps. Different subsystems are assumed to be independent. The assumption of independent subsystems is made in order to describe the solution in a closed form. It is acknowledged that a more sophisticated model is required in order to describe the effects of a closed national network in more detail. Nevertheless, the model proposed in this article extends the analysis of how a closed national network affects the operational capabilities in the overall system level. The closing process is a well-documented course of development as Russia is likely to implement 'RuNet 2020'. The model may be used to form and improve situation awareness as the process evolves. In order to further extend the analysis it is likely that one has to consider subsystems individually and allow them to be interdependent. Furthermore, one then has to also consider effects hierarchically, introduce network modelling and study time dependency. However, one may utilize parts of this study when further deepening the analysis as described.

Keywords: Modeling military capability, Modelling Critical Infrastructure, Cyber Domain, Closed Network Nation, Asymmetric Frontlines, RuNet

The first version of this paper was published and presented at the 17th European Conference on Cyber Warfare and Security (ECCWS), 28-29 June 2018, Oslo, Norway.

1 Introduction

In summer 2016, almost at the same time as NATO recognized cyberspace as a military domain, Russia declared that RuNet – the Russian segment of the Internet – would be disconnected from the global Internet by 2020; a system designated as 'RuNet 2020' (Ristolainen 2017, p. 114.). The de facto process of closing national networks is referred to as a closing process. The research has been continued in order to improve situation awareness of the closing process. For example, the military aims and impacts of the process have been analyzed. It was deduced that the military motivation behind Russia's network closing process is related to improving its military capabilities in cyberspace, namely traditional elements of combat power: protection, (relative) maneuverability and (relative) firepower. (Nikkarila and Ristolainen 2017.) Hence, the motive behind a closed network nation is to achieve higher operational capability than an 'open network society'. On the other hand, the motive for introducing RuNet may also be related to challenging the current world order. In the consequent research (Kukkola et al. 2017a/b/c.) it was revealed and analyzed how Russia is shaping the cyber battlefield in order to meet its aims. Russia's lines of effort were identified and in the research their outcomes were elaborated in the future cyber domain from the military viewpoint. It was stated that closing process creates a new type of cyber threat towards the remaining 'open network society' and in the earlier study (Kukkola et al. 2017b.) the need for further research in several fields in military science was emphasized and as well as deeper technical research. In military sciences further research is needed in the technical, tactical, operational and strategic levels. There is a need to construct models and scenarios in all these levels as well in order to form and develop situation awareness of the closing process. The situation evolves constantly and a clear picture of the whole closing process has not yet been formed; however it is seen that there is a will to form or strengthen alliances in cyberspace, an attempt to affect international norms and at least preparation of a state's own and allied systems in case international norms are not altered (Kukkola et al. 2017d, pp. 189-192).

In this study, we propose a system-of-systems model to describe the change in CND (Computer Networks Defence) -capability caused by the closing process and particularly the asymmetric frontlines between closed and open national networks. The capability is presented as a probability for denying adversarial operations in a friendly network. The closing process and the formation of asymmetric frontlines have an indirect effect in the CNA (Computer Networks Attack) and CNE (Computer Networks Exploitation) capabilities of a closed networks nation. However, CNA or CNE capabilities of a closed networks nation are not explicitly studied mathematically in the current research. The current study is the first system level mathematical model trying to describe the features of a closed national network e.g. in the perspective of the critical infrastructure of the closed network nation. However, the authors realize that the work has just begun and the present study serves as an intermediate step in trying to understand the ongoing closing process.

2 Potential Impact of the Closing Process

Potential outcomes of the closing process have been analyzed from an open network society's perspective and it was shown how a closed network nation is able to shape the cyber domain. The purpose of shaping the cyber domain is to gain an advantage and consequently, to control the cyber domain. There is a danger of open network societies being forced into a reactive mode. In the earlier study the choices of open network societies and their consequences were analyzed in the case of escalation and even a potential confrontation. Furthermore, the freedom of action of both the open and closed network nations is altered (Figure 1). (Kukkola et al. 2017a.)

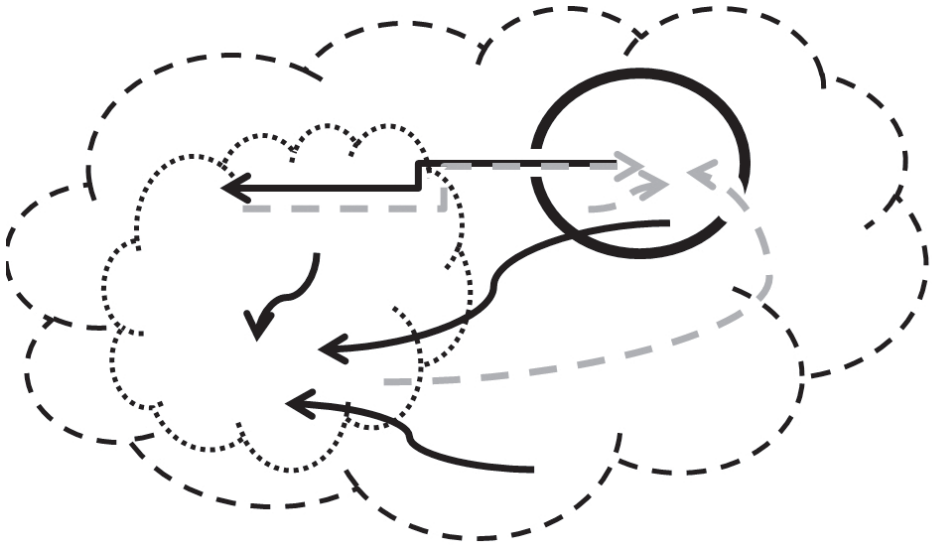


Figure 1. Schematic outline of open society network's asymmetry to a closed national network. The closed network is presented by a solid lined eclipse on the right and is enclosed by an open network society (i.e. the Internet). The dotted cloud represents an open national network. (Figure from Kukkola et al. 2017a).

Maybe one of the most interesting results of the closing process is the formation of asymmetric frontlines (Figure 2) in the cyber domain (Kukkola et al 2017b.). In the paper it was discussed how the fragmentation of the global network is progressing towards the formation of national segments of cyberspace. These national segments will be walled with 'digital borders' and will enforce the concept of digital sovereignty; e.g. by closing their national networks. In the earlier study, it was argued how the conventional asymmetry in cyberspace originating from the problem of attribution, is challenged or even made obsolete by the concept of digital sovereignty. It was demonstrated how 'digital sovereignty' is achievable by innovatively applying current technology and protocols. There is an obvious impact of digital sovereignty and the resulting asymmetric frontlines to the (near) future cyber battlefields.

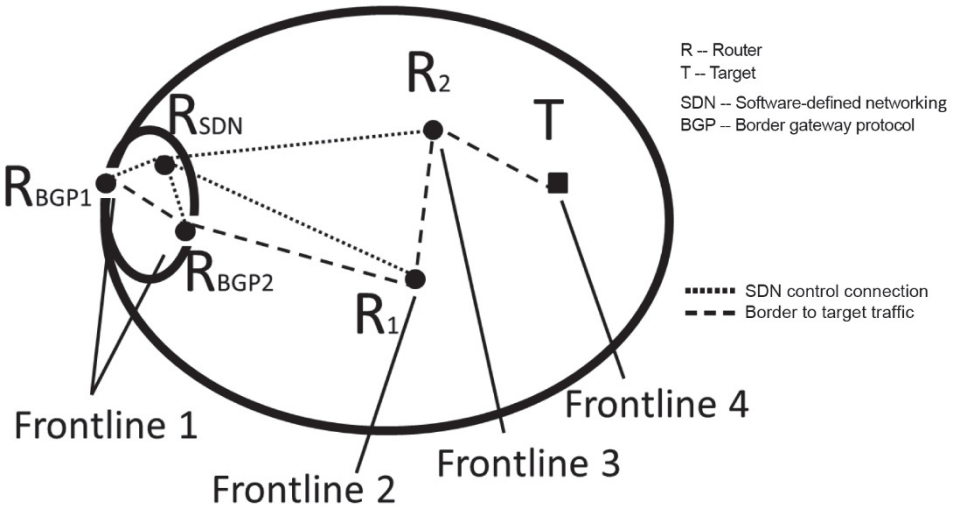


Figure 2. A simplified outline of the frontlines of a closed network. The largest eclipse represents the closed national networks and the smaller one demonstrates the government held border area. Since similar frontlines are absent in the open network it results in asymmetric frontlines. In the open national network all the safety measures are essentially conducted within or at the borders of the specific IT-system (marked as T=target in the figure). In the figure, one decision making router RSDN is actually a set of several routers that may be centrally controlled (Figure from Kukkola et al. 2017b).

In the study (Kukkola et al. 2017c) the potential impact of closing process was discussed as well. It was stated that its concrete outcome is the change in the freedom of action of closed and open network nations. Essentially, the outcome provides an ability to control escalation by forcing an opponent to react in a certain way by denying freedom of action or counterattacking. One of the end results may be that the closed network nation reaches escalation dominance over its potential adversaries. (Kukkola et al. 2017c)

3 Model Describing the Critical Infrastructure

As our current research is essentially a mathematical paper in its nature, we begin by introducing the most essential variables and notations in Table 1.

Table 1. Notations used in the paper.

Notation	Description
N	Total number of subsystems
M	Minimum number of operative subsystems needed in order to keep the total system operative
S_i	Steps to subsystem i
C_i	Capability of subsystem i, $C_i \in [0,1]$
$C(k)$	Total capability when k subsystems are operative
C_{tot}	Total CND capability
p_i	Probability of subsystem i being operative
$p_{i,normal}$	Probability of subsystem i being operative under normal conditions
$p_{i,s}$	Probability of successful CND operation of subsystem i at step s
δ_i	Variable indicating whether subsystem i is under attack, $\delta_i = 0$ or 1

Probabilistic models of war have been proposed in the literature (Cioffi-Revilla 1989; Cioffi-Revilla and Dacey 1988.). In this paper we use conditional probabilities to model asymmetric cyber-attacks and defense between closed and open national networks. The method is based on our earlier work on technology forecasting and capability modelling (Kuikka and Suojanen 2014; Kuikka et al. 2015a/b; Kuikka 2016).

Military capabilities can be modelled with basic probability theory using conditional probabilities. Our modelling is based on a system of systems concept, where a system can be described as parallel and serial sub-systems with a desired granularity. The highest level of modelling can comprise capability areas or a subset of functionalities from one or more capability areas. Functionalities are assumed to be independent – and if this does not hold, they should be further separated until the functionalities have no interceptions.

The general idea is to model the operation as multiple phases or levels. Typically, two taxonomies exist for the classification of attacks and defense actions. These two taxonomies may have common functionalities but usually the probabilities of success are different depending on the scenarios and other environmental factors (Suojanen et al. 2015.).

The derivation of the total capability is shown in the equations of Figure 3 and the derivation process is described below.

$$C_{\text{tot}} = \sum_{k=M}^{N} C(k) \tag{1}$$

$$\sum_{k=0}^{N} C(k) = 1 \tag{2}$$

$$C(k) = \Pr(K = k) = \sum_{A \in F_k} \prod_{i \in A} C_i \prod_{j \in A^c} (1 - C_j) \tag{3}$$

$$C_i = p_i \tag{4}$$

$$p_i = \begin{cases} 1 - \prod_{s=1}^{S_i} (1 - p_{i,s}), & \text{if under attack} \\ p_{i,\text{normal}}, & \text{otherwise} \end{cases} \tag{5}$$

$$p_i = \delta_i \left(1 - \prod_{s=1}^{S_i} (1 - p_{i,s}) \right) + (1 - \delta_i) p_{i,\text{normal}} \tag{6}$$

$$C_{\text{tot}} = \sum_{k=M}^{N} \sum_{A \in F_k} \prod_{i \in A} C_i \prod_{j \in A^c} (1 - C_j) \tag{7}$$

$$\begin{aligned} C_{\text{tot}} = \sum_{k=M}^{N} \sum_{A \in F_k} \prod_{i \in A} \left(\delta_i \left(1 - \prod_{s=1}^{S_i} (1 - p_{i,s}) \right) + (1 - \delta_i) p_{i,\text{normal}} \right) \\ \cdot \prod_{j \in A^c} \left((1 - \delta_j \left(1 - \prod_{s=1}^{S_j} (1 - p_{j,s}) \right) + (1 - \delta_j) p_{j,\text{normal}}) \right) \end{aligned} \tag{8}$$

Figure 3. Equations showing the derivation of the total capability C_{tot}.

In the following, we present the derivation process (shown in Figure 3) of the total CND capability C_{tot}. First, we assume that $C(k)$ fulfils the condition (eq. 1). Consequently, the probability of having exactly k operative subsystems out of N is given by the probability mass function of the Poisson binomial distribution (eq. 2). In the equation, F_k is the set of all subsets of k integers that can be selected from {1, 2, 3,…, N}. Symbol A represents the subset of elements belonging into F_k and A^C is the complement of set A. Notice that in the case that all C_i are identical (and thus C_j as well), the Poisson binomial distribution is simplified to equal the traditional binomial distribution. It is important to note that (eq. 3) is in practice infeasible to use, unless N is very small. Methods for computing $Pr(K=k)$ are presented in the Wikipedia article for the Poisson binomial distribution and its references. (Poisson binomial distribution)

Consequently, we *define* the capability of subsystem i as the probability of the system being operative (eq. 4). The probability of the system being operative is represented by (eq. 5) i.e. whether the system is under attack or not. Under normal conditions, the subsystem is operative with probability $p_{i,normal}$. When the subsystem is under attack, let $p_{i,s}$ be the probability of successful computer network defense operation of subsystem i at step s.

We define a variable δ, which is 1 when system i is under attack and 0 under normal conditions. Thus, the probability of the system being operative can be expressed as (eq. 6). Substituting the expression for the probability of k operative subsystems into the equation for total capability gives the form shown in (eq. 7), which basically shows the probability of at least M operative subsystems (i.e. the number of operative subsystems is on the interval $[M,N]$).

Finally, the total capability can be expressed as shown in (eq. 8), which is the main result of this article. It essentially gives the capability of the closed national network to protect the critical infrastructure of the closed network nation. The capability is expressed in a closed form as a total probability for at least a given number M (out of N systems) subsystems being operative under adversarial operation.

4 Simplified Example of Critical Infrastructure

In order to demonstrate the usage and usability of our model we present an example. We consider critical infrastructure with three subsystems of which at least two must be operative in order for the whole system to be

operative. The probability for each of the subsystems 1, 2 and 3 being operative is p_1, p_2 and p_3, respectively. The probability for all subsystems being operative is then simply $C(3) = p_1\, p_2\, p_3$ as given in equation (3). Similarly, the probability for any two of the three subsystems being operative is $C(2) = p_1\, p_2\, (1- p_3) + p_1\, (1- p_2)\, p_3 + (1- p_1)\, p_2\, p_3$. As a result, the total CND capability is of the form $C_{tot} = C(3) + C(2) = p_1\, p_2\, p_3 + p_1\, p_2\, (1- p_3) + p_1\, (1- p_2)\, p_3 + (1- p_1)\, p_2\, p_3$.

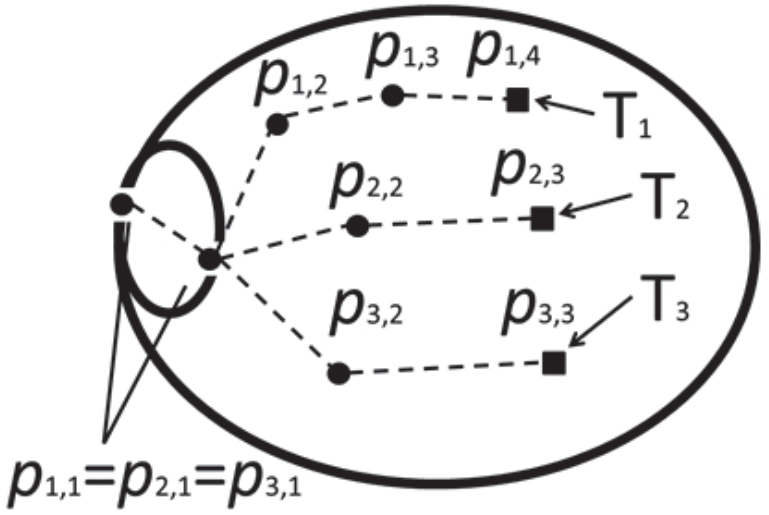


Figure 4. A schematic example of a simplified critical infrastructure within a closed national network is presented. Critical infrastructure consists of subsystems T1*,* T2 *and* T3*. Paths into each subsystem are shown in the figure.*

For the sake of simplicity, let us assume that all three subsystems are under attack. Consequently, $\delta = 1$ for all, $i = 1$, 2 and 3, and equations (5) and (6) are simplified. Furthermore, let us assume that the paths into each subsystem are as presented in Figure 4. In the figure, the paths into each subsystem T1, T2 and T3 go through the same border area and therefore, $p_{1,1} = p_{2,1} = p_{3,1}$. Consequently, the probabilities for each subsystem being operative, is presented in Table 2.

Table 2. Probability for each subsystem being operative.

Subsystem / C_{tot}	Probability p_i of the subsystem i being operative (ref: eq (5) and eq (6), and Figure 4)
T_1	$p_1 = 1 - (1 - p_{1,1})(1 - p_{1,2})(1 - p_{1,3})(1 - p_{1,4})$
T_2	$p_2 = 1 - (1 - p_{2,1})(1 - p_{2,2})(1 - p_{2,3})$
T_3	$p_3 = 1 - (1 - p_{3,1})(1 - p_{3,2})(1 - p_{3,3})$
C_{tot}	$C_{tot} = p_1 p_2 p_3 + p_1 p_2 (1-p_3) + p_1 (1- p_2) p_3 + (1- p_1) p_2 p_3$

As we want to demonstrate our model numerically as well, we assume numerical values of probabilities $p_{i,j}$ (i.e. the probability for successful CND operation at step j when the attacker tries to achieve subsystem i that is its target).

Table 3. We assume numerical values for successful CND operation at step j when the attacker tries to seek its target (i.e. subsystem i).

Subsystem path step	Numerical value of probability $p_{i,j}$
$p_{1,1} = p_{2,1} = p_{3,1}$	0.80
$p_{1,2}$	0.60
$p_{1,3}$	0.90
$p_{1,4}$	0.95
$p_{2,2}$	0.65
$p_{2,3}$	0.80
$p_{3,2}$	0.70
$p_{3,3}$	0.40

With the stated assumptions, the probabilities for successful individual CND operations and the total CND capability is shown in Table 4. It can be seen that the total CND capability is as high as 0.9995 (i.e. 99.95 %) even though some of the individual probabilities are rather low (e.g. $p_{3,3}$ =0.40). Essentially the result demonstrates the effect of asymmetric frontlines and concretizes how effectively a closed national network nation is able to protect its critical infrastructure. However, the authors would like to emphasize that all the given numerical values are purely assumptions and they do not have any direct or indirect relation with any nation's actual systems.

Table 4. Probability for each subsystem being operative and total CND capability (C_{tot}).

Probability p_i / total CND capability C_{tot}	Formula in numerical form	Numerical value
p_1	1 - (1 - 0.80)(1 - 0.60)(1 - 0.90)(1 - 0.95)	0.9996
p_2	1 - (1 - 0.80)(1 - 0.65)(1 - 0.80)	0.9860
p_3	1 - (1 - 0.80)(1 - 0.70)(1 - 0.40)	0.9640
C_{tot}	C_{tot} = 0.9996*0.9860*0.9640 + 0.9996*0.9860* (1-0.9640) + 0.9640*(1- 0.9860)* 0.9640 + (1- 0.9996)*0.9860*0.9640 = 0.950124 + 0.035482 + 0.013491 + 0.00038	0.9995

The results presented in Table 4 also show that in this case it is most likely that all of the subsystems remain operative (0.950124 of C_{tot}) under attack. The results also show that the most unlikely combination is that subsystem 1 is inoperative whereas subsystems 2 and 3 remain operative (0.00038 of C_{tot}). In other words, for the attacker this gives information that there is no point on using too much of its resources in order to bring subsystem 1 down. Instead, the attacker should concentrate on bringing down systems 2 and 3.

5 Conclusion and Further Studies

We have presented a system level mathematical model to describe how the cyber operational capability of a closed national networks nation is altered via the closing process. The model proposed in this research is a system of systems model representing the total capability of a closed national network in protecting e.g. critical infrastructure of the closed network nation. It is possible to analyze the effect on the military capabilities of the closed and open networks with the model. As a side result, we presented a definition for the CND capability as a total probability for the least required number of subsystems (of e.g. critical infrastructure) being operative under possible cyberattack. The closing process is a well-documented course of development and will be de facto in 2020 as Russia is likely to implement RuNet 2020. As the closing process continues, the understanding of it needs to progress as well. We are further developing the model and also otherwise constructing situation awareness of the process. We encourage the mathematical and scientific community in general to study the problem as well.

We also demonstrated our model numerically. With the given assumptions of individual probabilities we showed how the total CND capability can be quite high even though some of the intermediate steps give rather low probabilities. Essentially, we demonstrated how the asymmetric frontlines might result in surprisingly high CND capability. We also demonstrated how the model can be used in order to evaluate how difficult it is to bring down each subsystem. For both the defender and the attacker, this could be valuable information when planning the usage of their resources.

Related to our further studies, we acknowledge that in order to be more applicable the model has to be developed. However, we suggest that the proposed version of the model may serve as a starting point for further improvements. We argue that in order to extend the analysis it is likely that one has to study subsystems individually and consider their interdependency as well. One possible course of action is to analyze effects hierarchically, introduce network modelling and study time dependency. It is likely that the methodology will also then includeso simulations. However, one may utilize parts of this study when deepening the analysis as described. Also the parameterization work is significant when determining the probabilities of the intermediate steps of the model proposed in this research. To conclude, it is obvious that the amount of research needed just in the modelling field is substantial when trying to understand the effects of closed national networks.

References

Cioffi-Revilla, C. (1989) “Mathematical contributions to the scientific understanding of war”, *Mathematical and Computer Modelling*, Vol. 12, Issues 4–5, pp. 561-575.

Cioffi-Revilla, C., Dacey, R. (1988) “The probability of war in then-crises problem: Modeling new alternatives to Wright's solution”, *Synthese*, Vol. 76, Issue 2, August 1988, pp. 285–305.

Kuikka, V., Suojanen, M. (2014) “Modeling the Impact of Technologies and Systems on Military Capabilities”, *Journal of Battlefield Technology*, Vol. 17, No. 2, 9-16.

Kuikka, V., Nikkarila, J-P., Suojanen, M. (2015a) “A Technology Forecasting Method for Capabilities of a System of Systems”, *PICMET Conference*, 2015.

Kuikka, V., Nikkarila, J-P., Suojanen, M. (2015b) “Dependency of Military Capabilities on Technological Development”, *Journal of Military Studies*, Vol. 6, No 2.

Kuikka, V. (2016) “Number of system units optimizing the capability requirements through multiple system capabilities”, *Journal of Applied Operational Research*, Vol. 8, No. 1, pp. 26–41.

Kukkola, J., Nikkarila, J.-P., Ristolainen, M. (2017b) “'Asymmetric frontlines' of the cyber battlefields”, in *ICCRTS 2017*: *22nd Command and Control Research & Technology Symposium*, *November 6-8, 2017*, Los Angeles USA.

Kukkola, J., Nikkarila, J.-P., Ristolainen, M. (2017c) “Shaping Cyberspace: A predictive analysis of adversarial cyber capabilities”, in *IST-145/RSM-030 Specialists’ Meeting on Predictive Analytics and Analysis in the Cyber Domain, October 10-11, 2017*, Sibiu, Romania

Kukkola, J., Ristolainen, M., Nikkarila, J.-P. (2017a) “Confrontation with Closed Network Nation Open Network Society’s Choices and Consequences”, in *MILCOM* 2017: *Military Communications and Innovation: Priorities for the Modern Warfight, October 23-25*, 2017, Baltimore, MD, USA

Kukkola, J., Ristolainen, M., Nikkarila J-P (2017d) “GAME CHANGER: Structural transformation of cyberspace”, book (*Finnish Defence Research Agency Publications 10*) published by *Finnish Defence Research Agency*.

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

Poisson binomial distribution:
https://en.wikipedia.org/wiki/Poisson_binomial_distribution

Ristolainen, M. (2017) “Should ‘RuNet 2020’ be Taken Seriously? Contradictory Views about Cybersecurity between Russia and the West”, *Journal on Information Warfare*, Vol 16, no. 4, pp 113-131.

Suojanen M., Kuikka, V., Nikkarila, J-P., Nurmi, J. (2015) “An Example of Scenario-based Evaluation of Military Capability Areas – An Impact

Assessment of Alternative Systems on Operations", *IEEE International Systems Conference, April 13-15, 2015,* Vancouver, BC, Canada.

The Russian Segment of the Internet as a Resilient Battlefield

Juha Kukkola

Abstract

After the public demonstrations of 2011-2012 and the souring of relations with the West because of the illegal annexation of Crimea the Russian Federation has clamped down on Internet freedom. At first sight, this policy could be considered only as the reaction of an authoritarian regime to internal dissent and external propaganda. But after the publication of multiple government doctrines, programs and laws treating information security, and statements by the political leadership implying that Russia is planning to disconnect its national segment of the Internet it seems that something more is going on. This article claims that Russia is building a system-of-systems of cyber security and defence measures that it believes enables it to withstand cyber-attacks against its critical national assets. The subsystems of this entity have different functions and are controlled by various actors but can be joined to a centrally controlled system. This paper builds on previous research on Russian cyber strategy by aiming, firstly, to describe the developing national system-of-systems and, secondly, to analyse its effects on the resilience of the national segment of the Internet during peace time, intensified competition, conflict and war. The paper argues that the Russian Federation is aiming for a flexible, although complex and possibly vulnerable, national cyber defence system that could ultimately provide it a decisive advantage in a state-to-state cyber conflict.

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

The first version of this paper was published and presented at the ISMS Annual Conference 2018: "Military Sciences and Future Security Challenges", Warsaw, October 18th -19th 2018.

1 Introduction

After the public demonstrations of 2011-2012 and the souring of relations with the West because of the illegal annexation of Crimea the Russian Federation has clamped down on Internet freedom (Soldatov 2017; Freedom House 2017). Starting from 2014 the Russian Federation has issued laws limiting the freedom of the Internet in the country. Consequently, it published the Information Security Doctrine in 2016 which aimed to secure and control 'the national segment of the Internet'. The next year the Russian government adopted the Strategy on the Development of an Information Society in the Russian Federation for 2017-2030 and the state program of the 'Digital Economy' which among other things declared that Russia would achieve 'digital sovereignty' by 2020. In 2017-2018 the government published implementation plans on the 'Digital Economy' which stated that the Russian state would duplicate the most critical services of its national segment of the Internet and would ensure that by 2024 only 10% of the Russia's internal Internet traffic would go through foreign servers. Additionally, in 2017 Russia published a law on critical information infrastructure (CII) which aims to categorize national critical information infrastructure, obligates private owners to secure them and gives security services the mandate to monitor adherence to it. Moreover, Russia has been conducting state-level exercises to manage the disconnection of the national segment from the wider Internet from 2014.[1]

This article claims that what all these policies build up to is a system-of-systems[2] of cyber security and defence measures that Russia believes enables it to withstand cyber-attacks against its critical national assets. The project is a proof of the so-called fragmentation of the Internet that has been going on for some time now. This fragmentation is driven by some states, mainly authoritarian, who strive to create physically, logically and

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

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

semantically separated islands of the Internet that can be controlled by the state (Demchak & Dombrowski 2013; DeNardis 2014; Mueller 2017). The states have their various reasons for doing this, but this paper argues based on previous research that, at least partially, Russia approaches this process from the point of view of military strategy (Kukkola, Ristolainen & Nikkarila 2017). It is preparing the battlefield for a state-to-state cyber conflict. Russia might aim to gain a decisive advantage in this cyber conflict by centrally controlling, protecting and monitoring its national segment of the Internet and, if need be, by disconnecting it from the wider Internet.

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

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

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

uses mainly Russian sources and previous research conducted by the author and his colleagues.[5]

2 Confrontation and Resilience

The Russian concept of confrontation (*protivoborstvo*) characterises the Russian view on international relations. Russian theoretical thinking on information warfare divides relations into four stages: 1) 'peaceful coexistence' (*mirnoe sosushchestvovanie*); 2) 'conflict of interests' (*stolknovenie interesov*) or continuous 'natural rivalry' (*estestvennoe sopernichestvo*); 3) 'armed confrontation' (*vooruzhennaia konfrontatsiia*); 4) 'war' (voina) (Manoilo 2003, p. 276-277; Panarin & Panarina 2003, p. 20-21). According to Evgenii Shalamberidze, confrontation is more generally defined as "the actions of subjects of international relations to resolve their disagreements." It is divided into peaceful relations where non-violent means of confrontation are used; into foreign policy conflict where non-violent and violent direct and indirect non-military and indirect military means are used, and into military conflict where all means are used, primarily direct military (Shalamberidze 2011a, p. 28; Shalamberidze 2011b, p. 38-39). Chief of the General Staff of the Russian armed forces Valeri Gerasimov has presented a somewhat similar vision of the development of modern interstate conflicts or 'new type of war'. He emphasized the use of non-contact means against critical infrastructure objects in all dimensions of warfare (Gerasimov 2013). Later, General-Lieutenant Andrei Kartapalov argued that the West was preparing to use this 'new type of war' against Russia and Russia, as the weaker belligerent, should respond with 'asymmetric operations' i.e. using vulnerabilities of the enemy to negate its strength with minimal expenditure of resources (Kartapalov 2015, p. 35-36). Information means (including psychological and technological) are used in all phases of confrontation, but the use of open, kinetic or violent information means (i.e. cyber) increases when confrontation moves towards war. Russia should include counteracting these threats to its deterrence (*sderzhivanie*) (Dylevskii et al. 2016).

On the official side, the Russian military doctrine differentiates the national security situation between peace time, the time of immediate aggression, and war time (The Military doctrine of the Russian Federation 2014, p. 22).

---

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

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

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

In the framework of the Program of the Digital economy, resilience is related to the concepts of security, manageability and operational reliability (The Government of the Russian Federation 2018b). Security is related to the wider concept of information security which incorporates the protection

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

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

3 The System-of-Systems

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

[7] China's system is currently based on political censorship and societal control, and the state has controlled the development of the Internet from the beginning. Countries like Iran and Egypt have controlling mechanism based on technical solutions but do not have a comprehensive strategy for controlling the national segment of the Internet (Drake, Cerf & Kleinwächter 2016; Shires 2018).

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

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

The seventh system consists of state control of Internet traffic routing on physical and logical levels which aims to create the basis for a separated, and if need be closed, Russian segment of the Internet. This is achieved through direct state ownership of CII and through laws regulating the private sector. The system's function is to enable the closing of the national segment of the Internet (Kukkola & Ristolainen 2018).

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

4 The Battlefield

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

At the second phase of confrontation, a clear and present danger has emerged and operations against the national segment of the Internet have increased although the means used are still covert, indirect, and non-military. The situation might call for 'a state of emergency' or at least increased intervention of the state in the functioning of the Internet. Subsystems one and two are fully activated and subsystem three works in the background. Subsystems five and six are now activated in a centrally

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

controlled manner. They are used to monitor, counter and attribute aggressive operations. This increases the resilience of the national segment but additionally allows Russia, in the best case, to name-and-shame the attackers. The ability to monitor the rising threats against critical infrastructure and to counter exploitation operations (meant for future attacks) gives the state a definite advantage when individual private sector actors are not left alone to fend off attacks. It also provides a better situation awareness. This helps the state to prepare for potential future cyberattacks. At this point the national network is 'controlled' and has been prepared to withstand a wider and more aggressive attack and both technological and psychological effects are kept in check.

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

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

national segment are still resilient to a certain extent thanks to the modular nature of subsystems. At this point the national network is 'fragmented' but still resilient in its parts.

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

5 Conclusions

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

Resilience has become somewhat of a catchword in cyber issues since it was accepted that the attacker has the advantage. The only way to negate this advantage is to withstand the attack and recover as quickly as possible. If Russia manages to build up a system that allows it to do this on a national level, it will have a defined advantage. What is more important is that while its networks keep working and the psychological effects are negated,

aggressors might not have a similar advantage. This changes the balance of power in cyberspace. But what is perhaps more important is that the Russian system is explicitly based on an authoritarian view of the Internet. By copying it other states implicitly concede to Russian view of political relations in and between states. If the Internet is fragmenting, those states that want to uphold democratic freedoms must come up with a solution to this military-strategic challenge which does not lead them to give up their basic values.

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ross, Ron, Graubart, Richard, Bodeau, Deborah & Rosalie Mcquaid, 2018. Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. Draft NIST Special Publication 800-160 Volume 2 [Online]. Available from: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf [Accessed 13 June 2018].

Nye, Joseph S. Jr., 2011. The Future of Power. New York: PublicAffairs.
Panarin I. & Panarina L., 2003: Informatsionnaia voina i mir. Informatsionnoe protivoborstvo v sovremennom mire. Moscow: OLMA-PRESS.

Pilyugin, P., 2017. "Problemy opredeleniia granits v informatsionnom prostranstve", T-Comm: telekommunikatsiia i transport, 11(8), pp 37-44.
Rid, Thomas, 2013. Cyber War Will Not Take Place. London: Hurst & Company, 2013.

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

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

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

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

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

Shires, James, 2018. Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States. War of Rocks 12th October 2018 [Online]. Available: https://warontherocks.com/2018/10/between-multistakeholderism-and-sovereignty-cyber-norms-in-egypt-and-the-gulf-states/ [Accessed: 15th October 2018].

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

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

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

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

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

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

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

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

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

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

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

PLAYING THE GAME

Wargaming a Closed National Network: What are You Willing to Sacrifice?

Heikki Lantto
Bernt Åkesson
Juha Kukkola
Juha-Pekka Nikkarila
Mari Ristolainen

Abstract

Russia has a declared aim to close its national network from the global Internet. This could cause a situation where the rest of the 'open network society' is forced or wishes to consider closing their national networks as well. A situation where national governments substantially restrict information flows and connectivity of the network could cause serious effects to the critical infrastructure, economy, and alliances. This paper proposes a wargaming framework to analyze the effects of closing the national network on hostile actors operating critical infrastructure and who rely on the openness of that network for their operations. Our research provides information on what nations planning to close their network need to take into consideration while it offers a strategic insight for those actors who are confronted by a nation closing its network. This paper improves situation awareness and resilience in the cyber domain and supports global planning of cyber operations and defense.

Keywords: Cyber security, Resilience, Cyber defense, Wargaming, Closed national network, Critical infrastructure, RuNet

The first version of this paper was published and presented at the Conference for Military Communications (MILCOM), 29-31 October 2018, Los Angeles, CA, USA.

1 Introduction

Russia has declared its aim to close its national network from the global Internet and to become 'digitally sovereign'[1] by 2020 [1], [2]. Russia may, at the same time, be pursuing a decisive military advantage in cyberspace [3]. It seems that Russia is closing its national network in a controlled manner step by step and the 'closing process'[2] has been ongoing at least since 2014 [4]. The latest action plans for the period of 2017-2030 were published in January – February 2018 [5].

In this paper, we continue to analyze the possible impacts of Russia's network closing process on the remaining 'open network society'[3] [3]. Kukkola et al. [3] have shown that a 'closed network nation' will be able to force an 'open network society' into a reactive mode. Moreover, if Russia declares itself a 'digitally sovereign' nation it could cause a situation where an 'open network nation' might face closing its national network. Over the years, there have been many speculations of an 'Internet kill switch' that is a concept of activating a single shut off mechanism for all Internet traffic [6]. One could speculate, whether forcing an 'open network nation' into uncontrolled usage of such a kind of 'kill switch' might be one of Russia's strategic goals. A situation where national governments substantially restrict information flows and connectivity of the network could cause serious effects to its critical infrastructure, economy, and alliances [3].

In order to avoid a panic-like situation, we argue that it is necessary to analyze the decisions needed, i.e. to examine what kinds of issues the key

[1] 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 [29], i.e. cyberspace.

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

[3] 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. [28, pp. 221-238]. Open network nations share the values of open networks and their segment of the Internet is built on those principles. The open network society is the collection of the above defined nations.

actors[4] need to take into consideration when planning or being forced to close their national network. It is crucial to understand that the closing of a national network does not occur without sacrifices. The objective of this paper is to demonstrate the complexity and the ramifications of network closure. We show how wargaming offers a method for demonstrating and training to solve the problems that authorities involved could face. Moreover, through the wargame it might also be possible to reversely attain information of the strengths and weaknesses of a closed national network.

Firstly, for contextual and situational background the Russian process and understanding of the 'closed national network' is briefly explained. Secondly, a framework for the critical infrastructure of a generic state A is established for the design of the wargame. Thirdly, a wargaming framework in general is introduced as a method for extracting results. Fourthly, an exemplary set of wargaming scenarios of a chosen critical infrastructure is created in order to be matrix wargamed. The overall aim of this paper is to improve situation awareness and resilience in the cyber domain. Consequently, the goal is to support global planning of cyber operations and defense.

2 Closed National Network – 'RuNet 2020'

Over the years Russia has often expressed concerns about its national network's dependency on the global infrastructure and how the Internet 'can be switched off' from outside Russia's borders. There is a persistent 'rumor' in the Russian media that if Russia were to occupy, for instance, any European country, all Russian Internet connections would be disconnected within 24 hours [7], [8]. In 2014 the Russian government began to plan for disconnecting RuNet – the Russian segment of the Internet – from the global Internet and conducted a series of exercises to test its feasibility [9], [10], [11]. During the summer 2016, Russia declared that RuNet would be disconnected from the global Internet by 2020 [10], [11]. In the Information Security Doctrine, Russia openly aims to deploy a national system of managing the Russian segment of the Internet [1]. Likewise, 'sovereignty in the information space' was first officially mentioned in the Doctrine [1]. The main direction of information security is 'the protection of the sovereignty of the Russian Federation in the

[4] The concept of 'key actors' is defined in this paper as actors that are significant to the state. They include state authorities, critical parts of infrastructure and privately owned companies that deliver part of emergency supplies or produce a significant percentage of state Gross Domestic Product (GDP).

information space.' This will be achieved through non-conflictual and equal intergovernmental relationships. The Doctrine calls this state of affairs 'strategic stability.'

The Strategy on the development of the information society in the Russian Federation for 2017-2030, follows the Doctrine and takes a top-to-bottom approach to building a sovereign Russian information society [12]. Furthermore, the State Program of Digital Economy of the Russian Federation, tasks that Russia will be digitally sovereign by 2020 [2]. Additionally, a State Program 'Digital Information Society 2011-2020' states that Internet providers should be fully controlled by state regulation and 99% Internet resources registered by 2020 [13].

Disconnecting RuNet from the global Internet would launch a closed national network that has never been done before. It differs from the 'Great Firewall of China' both on the conceptual and the technical level. The Chinese system is more concentrated on censorship and is based on IP blocking, packet filtering, DNS blocking, URL keyword block, SSL MITN and VPN blocking [14], whereas RuNet is a more comprehensive system. There are a few Russian open source scientific studies on how to establish a closed national network and how it is related to achieving 'digital sovereignty' in practice. Border Gateway Protocol (BGP) combined with networking architecture Software Defined Networking (SDN) are introduced as probable (while not exclusive) technical solutions to implement a closed national network [15]. In the opinion of Kukkola et al., the most alarming fact is that the closing of a national network can most likely be executed with existing technology and protocols. It could be rather fast and relatively inexpensive to complete, when the political will has already been demonstrated in doctrines, strategies and state programs [3]. Considering the potential practical and technical solutions behind the Russian closed national network in parallel with recent Russian legal documents and changes in legislation, Kukkola et al. argue that the closing of a Russian national network is ongoing and it seems that over the next few years the Russian 'critical information infrastructure'[5] will fall under the control of Russian state authorities [3].

[5] Russian 'critical information infrastructure' includes for instance information systems and telecommunication networks belonging to government agencies, automated control systems for technological processes in the defence industry, and includes spheres of health care, transport, communications, financial institutions, energy, and fuel. Nuclear and aerospace industries, as well as a number of other areas, are also included on this list [3].

All the above mentioned indicates that Russia is closing its national network in a controlled manner and the 'closing process' is ongoing. Consequently, if a nation is able to plan and implement the closing of its national network it is better aware of the weaknesses of an 'open national network' than vice versa. Therefore, it is crucial for the entire 'open network society' to examine what kinds of issues need to be taken into consideration when closing or planning to close a national network. In this process it might also be possible to get reverse information on the strengths and weaknesses of a closed national network. Accordingly, in the following we simulate selected scenarios in the process of closing a national network in form of a wargame.

3 Critical Infrastructure of 'a Generic State A'

In general, 'critical infrastructure' refers to any system of high importance to the safety and operation of the country. Nevertheless, it is each government's definition that decides what is included in the 'critical infrastructure'. Obviously, there are terminological and conceptual similarities in how different countries use the concept of 'critical infrastructure'. In this paper, we use the European Union's definition and consider the 11 sectors of critical infrastructure as described in [16] as an example of classification of critical infrastructure (CI). As an example we use a 'generic state A' that either aims to close its national network or wants to prepare for unintended closure. In the wargame key actors are significant to the state and we demonstrate the consequences and possible decisions for them, to the state and to the actors related to them. We consider network traffic that crosses the national borders and the effect the closure has on it and on dependent functions and infrastructure.

A list of critical infrastructure sectors is shown in Table 1. There are complex interdependencies between the sectors and subsectors of CI. While recognizing and evaluating these interdependencies is important, it is outside the scope of this study. Instead, we focus on the influence of ICT on the other CI sectors, but do not provide an exhaustive set of dependencies. Our aim is to provide a framework for evaluating how changes to the ICT sector due to the closing process will impact the other sectors of critical infrastructure. In addition to critical infrastructure, we also need to consider the impact on non-critical infrastructure, national defense, public order and safety (government and public services, emergency services) and individual citizens. This is illustrated in Figure 1.

Table 1. Critical infrastructure sectors and subsectors

Sector	**Subsector**
I Energy	1 Oil and gas production, refining, treatment, storage and distribution by pipelines 2 Electricity generation and transmission
II Nuclear Industry	3 Production and storage/ processing of nuclear substances
III Information, Communication Technologies, ICT	4 Information system and network protection 5 Instrumentation automation and control systems (SCADA etc.) 6 Internet 7 Provision of fixed telecommunications 8 Provision of mobile telecommunications 9 Radio communication and navigation 10 Satellite communication 11 Broadcasting
IV Water	12 Provision of drinking water 13 Control of water quality 14 Stemming and control of water quantity
V Food	15 Provision of food and safeguarding food safety and security
VI Health	16 Medical and hospital care 17 Medicines, serums, vaccines and pharmaceuticals 18 Bio-laboratories and bio-agents
VII Financial	19 Payment and securities clearing and settlement infrastructures and systems 20 Regulated markets
VIII Transport	21 Road transport 22 Rail transport 23 Air transport 24 Inland waterways transport 25 Ocean and short-sea shipping
IX Chemical Industry	26 Production and storage/processing of chemical substances 27 Pipelines of dangerous goods (chemical substances)
X Space	Space
XI Research	Research facilities

The wargame examples are based on this framework and their purpose is to support decision makers with information regarding the impact of the closing process and to highlight the issues that would arise. Moreover, this kind of framework could provide a view about nations' necessary decisions or actions required in order to close their national networks or prepare for the closure. We emphasize the need to understand the sacrifices needed in order to obtain a closed national network and its potential benefits. We argue that wargaming can be applied in order to extract the necessary information in order to manage the addressed complexity of the closure.

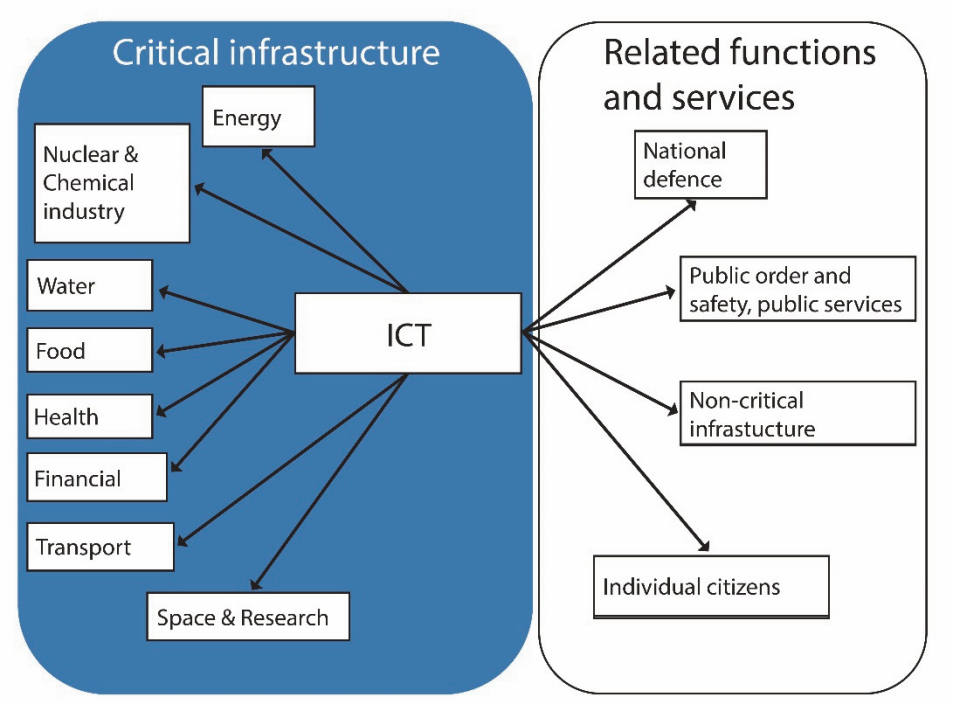


Figure 1. Relation of ICT to critical infrastructure and other functions and services.

4 Wargaming

The military has used wargaming as a tool for warfare at least since the Roman Empire [17] or Sun Tzu who is credited for creation of game known as Wei Hai [18]. Wargaming has been an important and powerful tool for training, education, research, and refining plans [19], [20]. The assumption has been that wargames provide an opportunity for militaries to make decisions and to learn about the effects of those decisions [17], [18]. Wargaming in the broadest definition includes nearly any analytical method for exploring potential outcomes to a given situation [20], [21].

When wargaming works it can give a lot of information and experience on the subject [19]. By creating for its participants a synthetic experience, wargaming gives them palpable insight that helps them better prepare for dealing with complex and uncertain situations in the future [19]. The goal of wargaming is to generate enough discussion so that general gaps could be identified [22]. Wargames are very useful for uncovering "black swans" or unforeseen events, for example in current cyber defenses [22].

The need to explore, repeat, and reflect on decisions made in the context of wargames is critical for what we must do to learn better how to cope with a world rapidly moving beyond our range of real experiences [19]. Wargames are synthetic experiences that give players active responsibility for their decisions, similar to what they would experience in the real world, and force them to bear many of the same consequences of those decisions [19]. A successful wargame should portray a realistic set of outcomes and reactions, and generate insights for the participants [22]. Wargaming is not a way to predict the future and it is not, in itself, an analysis. However, conducted with clear goals and a definite scope, it can produce outputs that support the work conducted by analysts in providing actionable information [23].[6]

Wargames are severely affected by trade-offs between accuracy and simplicity as a wargame is a synthetization of several modelling approaches. Human behavior is too complex and unpredictable to shrink into one simple model [24]. A computer program can handle many of the details, such as calculating complex psychological factors, as well as providing artificial intelligence agents to run the opposition force. Manual games provide a human dimension as players interact with each other [25]. It was recognized that in complex, human environments, an approach that prioritizes useful abstraction over exhaustive simulation is more likely to produce analytically useful outputs [23].

The traditional conception of a wargame involves two teams (the blue team representing the home country and the red team as the opposition force), playing out an outgoing scenario over a series of moves [23].. Alternatively, the game mechanics itself may simulate adversarial actions while the players are on the same side.

Matrix games are different to normal games. In most of those games you compare lists of statistics and rules to describe what should happen [26]. In matrix games statistics and rules are replaced with a process of guided argumentation between players [23], [27]. The aim is to encourage the exchange of ideas and views to develop a deeper understanding of a topic [26]. Games help to develop the participants' understanding of complex situations. They are very simple to set up, require a minimum of components and don't take very long to play [27].

[6] Of course, wargames can also give players false beliefs and assumptions in any number of ways.

Matrix games use words to describe why something should happen, the umpire decides how likely it is and makes judgement, maybe assisting judgement by rolls of dice. If a player can say something happens and why it happens, they can play a matrix game. Generally each argument in a matrix game is broken down to an argument (something that happens) and reasons why or how it happens. A strong and knowledgeable umpire is the key to running a successful game.[7]

Wargame designers have a responsibility to avoid many of the common mistakes that organizations make when they consider future challenges [19]. These errors include both presenting mistaken information or under- or overstating the dangers involved in these events [19]. Wargames are only reliable in selected features of the real world [20], [23]. The key question in the design of any wargame intended to be used to consider real-world problems is to ensure that it models the factors that are relevant to its requirements [23]. A dedicated wargame is needed if threats are to be identified [22].

Crucial to the design of the wargame is that the participants are subject-matter experts. This reduces the level of pre-reading and briefing required for the participants in the wargame [23].

5 How to Study Consequences of Closing a National Network?

Obviously, there are many issues worth considering in the closing process. These issues are essential for the decision makers in making their decisions. In this paper, we use as an example 'a generic state A' that closes its national network either intentionally or unintentionally. We present a logic for considering issues and give an idea of the required level of detail. In practice, we present three examples which aim to demonstrate the complexity and the interdependencies of the problem. We argue that in practice it is impossible to study the entirety of the closing process inclusively. Therefore, it is necessary to examine the process in pieces. Consequently, we have created a representative set of scenarios. Since the particular interest is the effect for state A, we have formed three scenarios representing the general situation of state A. Each scenario forms the basis

[7] A good example of matrix game in complex inter-relationships of cyber warfare is presented in the Curry and Price book of Dark Guest Training Games for Cyber Warfare: Volume 1 Wargaming Internet Based Attacks [26].

of a matrix game. The first scenario is explained in more detail and the following two demonstrate the complexity of the process.

In all scenarios, the initial player is the one whose processes are directly affected. The authors acknowledge that the scenarios are exemplary and schematic. Their role is to demonstrate how matrix wargaming could be applied in practice to investigate the impacts of the closing process. The aim is not to give a detailed description of the wargame. In an actual wargame the closing process should be divided into multiple layers, and interdependencies between all the subsectors ought to be considered. All scenarios begin with the decision to cut off the network connections crossing the border of state A. The umpire describes the situation at the beginning of the game turn. The initial player presents the immediate effects within their area of responsibility and the action they will take, along with the reasons and the required time frame. The other players will present their own actions within the set time frame with arguments for their actions and within their own scopes. The players may share some of the objectives of the initial player, and may support their operations within their abilities or may impose restrictions. Since some of the objectives are common, the players may cooperate and try to find a consensus regarding the required time scale. Based on the arguments made by the players, the umpire decides the immediate outcome and the next time step and starts a new game turn. The game continues until the initially set objectives have been achieved or the game has reached a point where the situation no longer evolves. The end results are collected and the final conclusions are drawn. Of particular interest are the consequences for the initial player i.e. for state A.

5.1 Example 1: Private business related to CI (Health sector) of state A

Scenario 1 (shown in Figure 2) consists of a highly important (and multinational) pharmaceutical company *a* operating within state A. The company has an important role in state A with a connection to the state's emergency supplies. It generates a substantial percentage of the national GDP as well. As the firm in question is multinational its ICT is divided across several countries, with inventory accounting located in another nation (state B). Furthermore, there are a substantial number of connections into state C as the company billing is located there in a bank *c*, and an important subcontractor is based there as well. For example, one of the first issues the players have to solve is how they communicate with each other when the Internet connections are cut off.

The players in this scenario are subject matter experts with the following roles: companies *a*, *b*, *c*, *d*; the authorities in A; ICT partly in A; other players as required. Players may play multiple roles. Player *a* is the initial player.

Player *a* lists all the implications of losing the connections with its inventory, billing and subcontractor, and reasons them accordingly. He will also present the immediate action to mitigate the situation. A successful mitigation is likely to require actions to be conducted by the other players *within a certain time frame* given by player *a*. The other players will then present their reasoned responses and address which actions can be conducted within the time frame set by the player *a*. The game turn is ended by the final umpire decision regarding to the immediate outcome. As the umpire is aware of the time frame important especially to company *a* he/she decides the next time step and starts a new game turn.

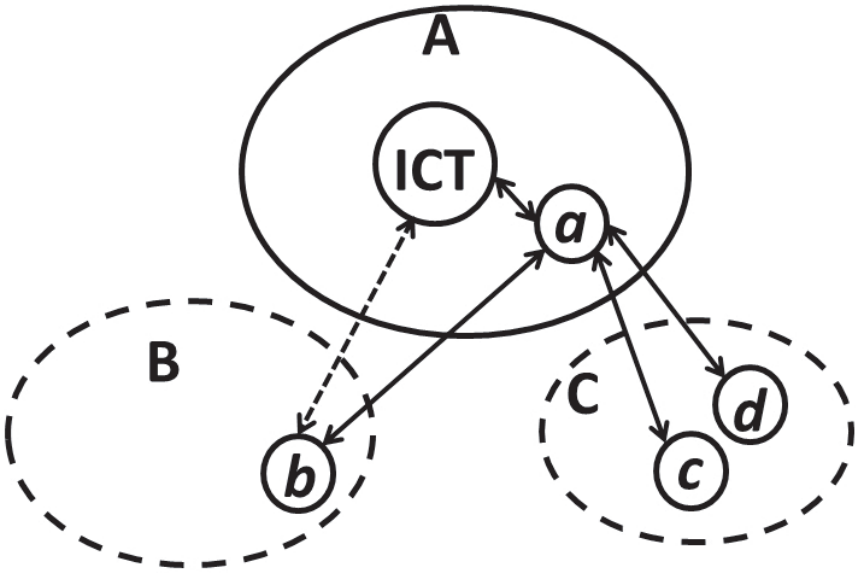


Figure 2. Example of a privately owned multinational company related to CI (Health sector) of state A. Figure shows schematically the cross-border connections crucial for the company being operative.

At the beginning of the next game step, *a* describes briefly if the outcome of the previous time step is satisfactory or if the new situation consists of existing or further issues that have to be addressed. Otherwise the game step is played similarly to the previous one. It is important to note that the possible interdependencies are considered explicitly as the actions conducted within the preceding time step have altered the initial situation

of the current time step. Furthermore, the actions conducted during the current time step affect the initial situation of the following time step.

The game continues until it has reached a point where the situation no longer evolves. The final outcome may consist of the economic effects, changes of the company *a* sites' locations, the company's capability to provide emergency supplies and possible changes to its initial and current business partners.

5.2 Example 2: A subsidiary (later: a bank) of an international banking company located in country A

Scenario 2 (shown in Figure 3) consists of an international banking company with headquarters located in state C and a subsidiary based in state A. The bank's customers are mainly domestic, but there are several connections with several other banks in different states. The connections are complex consisting of interdependent loans, money transfers etc. The bank is also connected to the stock exchange in country A. There are several servers, owned or held by the bank within country A, but certification may cross the border.

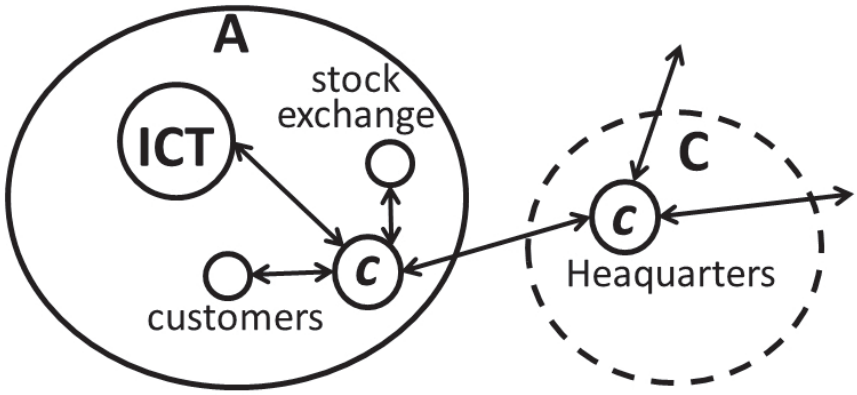


Figure 3. Financial-related example of a banking company operating in state A. The figure shows schematically the cross-border connections crucial for the company to operate.

The players in this scenario are subject matter experts with the following roles: company *c*; the authorities in A; ICT partly in A; other players as required. Stock exchange and customers may be played by player c. Player

c is the initial player and the game is played until the situation has stabilized or the objectives of the scenario have been achieved. One of the main objectives is to resolve whether or not the bank is able to operate in state A and to estimate the level of possible economic losses.

5.3 Example 3: National authority of country A with a database (a register) outsourced abroad

The players in this scenario are subject matter experts with the following roles: the national authority; the cloud service provider; ICT in A; other players as required. The national authority is the initial player.

The National authority of country A has subcontracted some of its services (records/databases) to an international cloud service provider in country B, the country establishing a closed national network. In this game, the national authority in question of state A would be the first player.

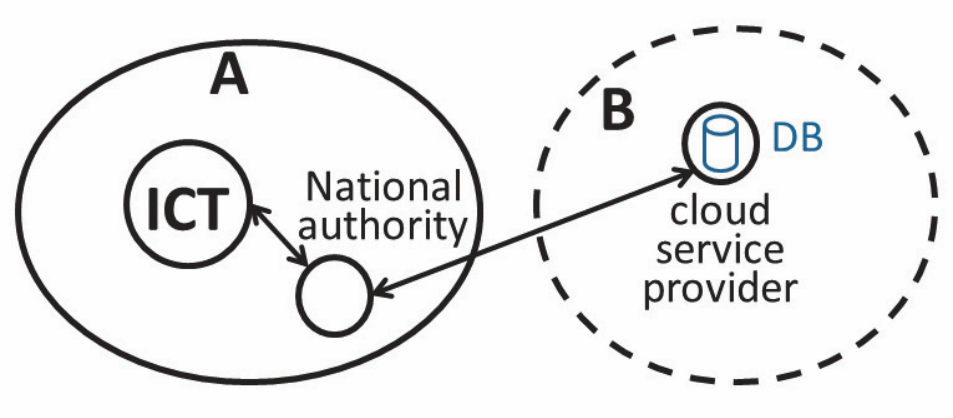


Figure 4. Schematic figure of a situation where a national authority of state B has outsourced one of its registers (DB=data base) to a cloud service provider that operates in state A. The figure shows schematically the cross-border connections between the authority and its register.

When the national networks are closed it brings up the immediate issues and how they could be mitigated. The other players: cloud service provider, ICT and possibly national authority of state B would propose how they might be able to address the problem. A possible outcome of the game could be that the authority (of state A) may not be able to access its records (problem in availability). The service cloud provider possesses the data physically without the national authorities of the state B being able to guarantee the secrecy of the data (problem in confidentiality). Even if the

data could be extracted from the database its integrity might be uncertain. Depending on the level of sensitivity of the data a network closure could lead to concerns of national security.[8]

6 Discussion

In this paper, we have presented how the consequences of closing national networks can be studied by using matrix wargaming methods. Wargaming can be used as a means to convey the complex interdependencies and interactions to decision makers. Whether the closing of national networks is intentional or unintentional, the consequences need to be studied comprehensively to avoid potentially disastrous courses of actions and unanticipated end results. One observation is that the proposed method could be used in order to prepare the decision makers for the complexity of such possible ramifications and their impacts. The method demonstrates the issues that have to be addressed before closure. In other words, by applying the method one may recognize the weak points of ones' own systems and networks. The game could be used to observe, detect and avoid courses of action that are disastrous to one-self.

Extracting any consistently produced information of the impacts of a national networks closure is important. By wargaming one may get a hint of the thinking of decision makers of states that have chosen to close their national networks. By wargaming one may even be able to extract the sacrifices made by such states. If the sacrifices were revealed one would be able to evaluate whether or not those sacrifices were acceptable to the key actors and furthermore, to the state.

Additionally, one could even avoid making those sacrifices unintentionally. Knowing beforehand the unfavorable courses of action is of high importance. Especially when countering an adversary's deception that aims to divert our reaction into a direction favorable only to the adversary. Moreover, by utilizing the proposed method one may demonstrate the effects of the inoperability of the national networks for any reason: e.g. major natural disasters, large-scale hack campaign or hacktivism, or a sudden electricity loss (for example due to a geomagnetic storm).

[8] E.g. the Swedish Transport Agency's vehicle and license records in the news in 2017 [30].

To conclude, we propose to wargame the closing of national networks even if, and especially if, a state is not actually willing or aiming to close their national networks.

References

[1] "Doktrina informatsionnoi bezopasnosti Rossiiskoi Fereratsii [Information Security Doctrine of the Russian Fereration]," 5 December 2016. [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf. [Accessed 27 December 2016].

[2] "Programma:"Tsifrovaia ekonomika Rossiiskoi Federatsii" [State Project: Digital Economy of Russian Federation]," 28 June 2017. [Online]. Available: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf. [Accessed 3 August 2017].

[3] J. Kukkola, M. Ristolainen and J.-P. Nikkarila, Game Changer: Structural Transformation of Cyberspace, Riihimäki: Finnish Defence Research Agency, 2017.

[4] M. Ristolainen, "Should 'RuNet 2020' be taken seriously?," Journal of Information Warfare, vol. 16, no. 4, pp. 113-131, 2017.

[5] J. Kukkola, "Research Bulletin: New guidance for preparing Russian 'digital sovereignty' released," Finnish Defence Research Agency, Riihimäki, 2018.

[6] D. B. Medows, "The Sound of Silence: The Legality of the American "Kill Switch" Bill," Journal of Law, Technology & the Internet, vol. 4, no. 1, pp. 59-79, 2012.

[7] D. Nazarov, "Rezervnaia kopiia: Mozhno li otkliuchit' rossiiskii internet ot global'noi seti? [Back-Up-Copy: Can the Russian Segment of the Internet be Disconnected from the Global System?]," 1 September 2016. [Online]. Available: http://www.furfur.me/furfur/freedom/freedom/218695-chto-takoe-rezervnaya-kopiya-interneta. [Accessed 4 October 2016].

[8] R. Rozhkov, ”Pervye litsa: ”Internet ”liazhet” na sutki? Ia etogo voobshche ne ponimaiu” Gendirektor TTSI Aleksei Platonov,” Kommersant', 18 March 2016.

[9] R. Oliphant, “Russia 'tried to cut off' World Wide Web,” 15 October 2015. [Online]. Available: http://www.telegraph.co.uk/news/worldnews/europe/russia/11934411/Russia-tried-to-cut-off-World-Wide-Web.html. [Accessed 19 October 2016].

[10] A. Sukharevskaia, "Zapasnoi internet: Kto zaimetsia sozdaniem ”reservnoi kopii” [Spare Internet: Who Will Establish the “Back-Up-Copy”]," RBK: ezhednevnaia delovaia gazeta, 7 July 2016.

[11] A. Sukharevskaia and I. Iuzbekova, "Tri voprosa o suverennom runete [Three Questions about Sovereign RuNet]," RBK: Ezhednevnaia delovaia gazeta, 6 June 2016.

[12] "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. [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf. [Accessed 24 July 2017].

[13] Minkomsviaz, “Gosudarstvennaia programma ”Informatsionnoe obshchestvo” (2011-2020 gody), [State program “Information Society” (2011-2020)],” 27 August 2014. [Online]. Available: http://minsvyaz.ru/ru/activity/programs/1/. [Accessed 12 April 2018].

[14] N. Inkster, China's Cyber Power, London: The International Institute for Strategic Studies , 2016.

[15] A. Streltsov and P. Pilyugin, “K voprosu o tsifrovom suverenitete [About digital sovereignty],” Informatizatsiia i sviaz', no. 2, pp. 25-30, 2016.

[16] Comission of the European Communities, "Green Paper on a European Programme for Critical Infrastructure Protection," European Union, kaupunki puuttuu, 2005.

[17] A. Frank, Gamer mode: Identifying and managing unwanted behaviour in military educational wargaming, Stockholm: KTH Royal Institute of Technology, 2014.

[18] P. P. Perla, The Art of Wargaming: A Guide for Professionals and Hobbyist, 1990., Annapolis: Naval Institute Press, 1990.
[19] P. P. Perla and E. McGrady, "Why Wargaming Works," Naval War College Review, no. 64, pp. 111-130, 2011.

[20] M. Hanson, Improving Operational Wargaming: It's All Fun and Games Until Someone Loses a War, Fort Leavenworth: United States Army Command and General Staff College, 2016.

[21] M. Van Creveld, Wargames: From Gladiators to Gigabytes, New York: Cambridge University Press, 2013.

[22] E. Colbert, D. Sullivan and A. Kott, "Cyber Wargaming on SCADA Systems," in Proceedings of the 12th International Conference on Cyber Warfare and Security (ICCWS 2017), Reading, Academic Conferences and Publishing International Limited, 2017, pp. 96-104.

[23] N. Ashdown, "Analysts use gaming to study Syrian conflict," Jane's Intelligence Review, no. February 19, 2016.

[24] P. Sabin, Simulating War: Studying Conflict through Simulation Games, London: Continuum, 2012.

[25] J. Miranda, "Wargaming the Cyber Frontier," in Zones of Control, Cambridge, The MIT Press, 2016, pp. 673-680.

[26] J. Curry and T. Price, Dark Guest Training Games for Cyber Warfare: Volume 1 Wargaming Internet Based Attacks, lulu.com, History of Wargaming Project, 2013.

[27] J. Curry and T. Price, Matrix Games for Modern Wargaming, lulu.com, lulu.com, 2014.

[28] N. Choucri, Cyberpolitics in International Relations, Cambridge: MIT Press, 2012.

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

[30] C. Anderson, "Swedish Government Scrambles to Contain Damage from Data Breach," The New York Times, 25 July 2017. [Online]. Available: https://www.nytimes.com/2017/07/25/world/europe/ibm-sweden-data-outsourcing.html. [Accessed 30 April 2018].

Wargaming the Cyber Resilience of Structurally and Technologically Different Networks

Heikki Lantto
Simo Huopio
Bernt Åkesson
Juha-Pekka Nikkarila
Marko Suojanen
Mari Ristolainen
Topi Tuukkanen

Abstract

Based on a review of different analytical frameworks, a table top cyber wargame is suggested to be applied when trying to analyse the effects closed national networks may impose in the near future. The scope of the wargame is to extract results of how the resilience of an open national network differs from a closed national network. It is self-evident that the formation process of resilience is different between the diverse systems. The proposed wargame is a two-sided cyber table top wargame. The wargame is based on at least two blue teams, at least one red team and a control team (namely a white team). One blue team is located in the closed national networks and its system relies on closed national network infrastructure. The other blue team operates its system within an open network society. By designing, constructing and executing the proposed cyber wargame we argue it is possible to find these differences and similarities as well. Current research improves cyber situation awareness and proposes a direction to follow when trying to understand the changing circumstances of cyber space. It also gives a suggestion as to how research resources could be directed when trying to improve situation awareness of the closing process.

Keywords: Cyber Defence, Cyber resilience, Wargaming, Closed national network, Russia

The first version of this paper was published and presented at the ISMS Annual Conference 2018: "Military Sciences and Future Security Challenges", Warsaw, October 18th -19th 2018.

1 Introduction

Earlier it has been shown that Russia has initiated a network closing process that aims to improve its cyber capabilities when compared to its adversaries. Essentially, by 2020 Russia aims to achieve the capability to monitor, control, restrict, and if necessary close the Russian segment of the Internet. If the closing process is successful technically, this would cause significant structural changes in cyberspace and create an asymmetric advantage (Kukkola *et al*. 2017b). Allegedly, the cyber resilience of a closed national network[1, 2] (Kukkola 2018) is different than the remaining open network[3]. Moreover, this resilience may invoke intended or unintended aspirations to shape cyberspace to a state's own benefit and could potentially lead to haphazard and even dangerous international political endeavours if unchecked. This paper seeks to develop an analytical approach to evaluate the differences between a closed national network and the open network. Based on our analysis, the initial research could be based on wargaming, providing sufficient ground for later expansion of similar research efforts.

In 2014, the Russian government began to plan for technical disconnecting the Russian segment of the Internet (RuNet) from the global Internet (if needed) and conducted a series of exercises to test its feasibility. During summer 2016, Russia declared that RuNet would be capable of being disconnected from the global Internet by 2020. (Kantyshev and Golits'na 2016) Moreover, Russia aims at technological self-sufficiency and wants to reduce its dependence on imported technology. In addition, there are several countries that wish to question and challenge the US-dominated/led

[1] 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 technically separated from the global Internet. The concept is used without quotation marks hereafter.

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

[3] 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. (Choucri, N., 2012, pp. 221-238). Open network nations share the values of open networks and their segment of the Internet is built on those principles. The open network society is a collection of the above defined nations. The concepts open network, open network nation and open network society are used without quotation marks hereafter.

world order, i.e. both structurally and technologically different networks are emerging in the future. Consequently, it is important to analyse how the features of closed national networks differ from the open society networks at the technical, tactical, operational and strategic levels. (Kukkola et al. 2017a)

Starting from the application of versatile technologies, the actor that owns a closed national network has had many alternatives for implementing the network. Since security and isolation of the network have been the primary design drivers, the excessive expense of building proprietary networks of domestic origin is only a secondary factor. For other actors relying on open network technologies, technology selection and building of network-centric and command & control capabilities is hindered by the requirements of the need to connect everything, interoperability, limited technology alternatives from major communications technology providers and all other consequences that follow from picking up those technologies e.g. operating systems, application interfaces and connection alternatives. Using open source software and open architectures improves interoperability, and communities of active cyber experts may improve cyber security of those systems by seeking and advertising cyber vulnerabilities, but at the same time key elements of these open networks are available on the Internet to all actors. Therefore, an actor that owns the closed national network has an upper hand over the other that relies on the open network, since there may not be similar access points as the open network has. Also, as the network structure, technologies, redundancies, encryption, use cases, procedures and even actors may be unknown beforehand, the owner of a closed network is many steps ahead in protection of the network in contrast to the owner of the open network. The initial steps for finding out the first access point requires extensive pre-analysis based on information that may not be collected in any other way than getting physically close to the network. Even though part of the network would be investigated physically, the whole closed network might still be built on versatile technologies and different procedures to access services that would make it complicated for adversaries to accomplish cyber activities in this unknown network. (Kukkola et al. 2017b)

2 Analytical Frameworks

As researchers (Kukkola et al. 2017b) allude to, the Russian initiatives, inter alia the Runet 2020, may have, at least in the background, aspirations which can easily be framed under the concept of cyber power. (Nye 2011) Within cyberspace, the relative low costs involved, challenges of

attribution and inherent asymmetries due to vulnerabilities have led to a situation where ever smaller belligerents have the potential to exercise tools and leverages related to the notion of cyber power. The notion of power itself, however, has been challenged. The interpretations of the definition and constituent elements differ from one stakeholder to another based on their interests and values. Moreover, the notion is highly dependent on the context. However, in order to direct our focus, we shall adopt the following definition (Kuehl 2009, in Kramer et al. 2009):

"Cyber power is the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."

This definition is most appropriate for our purposes of considering how the Russian initiatives are about to change cyberspace and to influence potential future events. However, with the potential evolution of these, we do not yet have clearly defined context. Therefore the concept of cyber power would, at the moment, be an overkill for our academic scrutiny exploring potential outcomes of implementation of these Russian initiatives.

Another avenue we could approach to analyse the Russian initiatives could be through the notion of national cyber security, which is widely used in contemporary policy discussions, yet partly undefined and significantly influenced by the individual national context. (Klimburg 2012) starts with the notion of national cyber security as:

"National Cyber Security is the focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security."

Based on this definition he further presents a theoretical framework to analyse national cyber security consisting of:

1. The five mandates: military, intelligence, counter cybercrime, critical infrastructure protection, and cyber diplomacy
2. The three dimensions: governmental, national, international
3. The five dilemmas: economy vs. security, modernization vs. protection, private vs. public sector, data protection vs. information sharing, freedom of expression vs. political stability.

We recognise that the Russian initiatives could well be analysed through this theoretical framework. However, to do so would involve a much more elaborate research program than currently available to the authors.

Within the defence planning domain, capability based planning has proliferated since the demise of the Cold War. Capability as a term has different definitions and meanings in different contexts, similarly to what we have already seen earlier in this paper. In a military context, capability sometimes refers to objectives, tasks needed to achieve these objectives, or means of conducting these tasks. The concept is used by various stakeholders and in different levels of planning, which has led to the emergence of a number of capability models within the western military context. However, we shall consider adopting the Comprehensive Capability Meta Model (CCMM). (Anteroinen 2012) The CCMM presents a horizontal definition of the primary application area of the capability perspective, the stakeholders, relevant process, temporal features and the motivation of each capability perspective. Within the model:

1. The CCMM level 1 defines the scope. For our purposes we shall label this as Cyber Power. At the national level, the cyber capabilities represented by the notion of Russian Information Security are seen as an element and an instrument of foreign policy. Consequently, this capability level is one of the elements in international relations.
2. The CCMM level 2 defines the business model. At this level the capability is seen as an ability or a capacity to perform a set of tasks, or an ability to achieve a desired effect. This functional, or business, model is used in planning to avoid potential bias towards a particular solution and to develop solutions suitable for a wide range of operations.
3. The CCMM level 3 defines the system model. The military acquisition process often sees capability as systems. In this perspective, capability is a conceptual system defining the components of that capability. The system model can also be viewed through different capability lines of development known as DOTMLPFI, where D stands for doctrine, O for organization, T for Training, M for materiel, L for Leadership, P for personnel, F for facilities and I either for information or Interoperability.
4. The CCMM level 4 is defined through a technology model. The capability is typically seen by the system operators and developers as a technical system or a platform. This technology perspective describes the components of capability rather than the capability itself.

5. The CCMM level 5 is a detailed representation of sub-systems. The sub-systems viewpoint is used to decompose the systems or platforms into modules or sub-systems. Anteroinen (2012) argues that this detailed representation perspective is crucial in the realization of the capabilities aspired to.
6. The CCMM level 6 depicts the functioning enterprise. As this is probably the most obvious and visible capability viewpoint, it can be viewed as the ability to control the Russian Internet and for federal organizations to manoeuvre in international cyberspace.

These CCMM levels form an interdependent network of capability views where some views may manifest themselves as real life instances whereas some are more abstract as depicted in Fig. 1. (Koivisto and Tuukkanen, 2017)

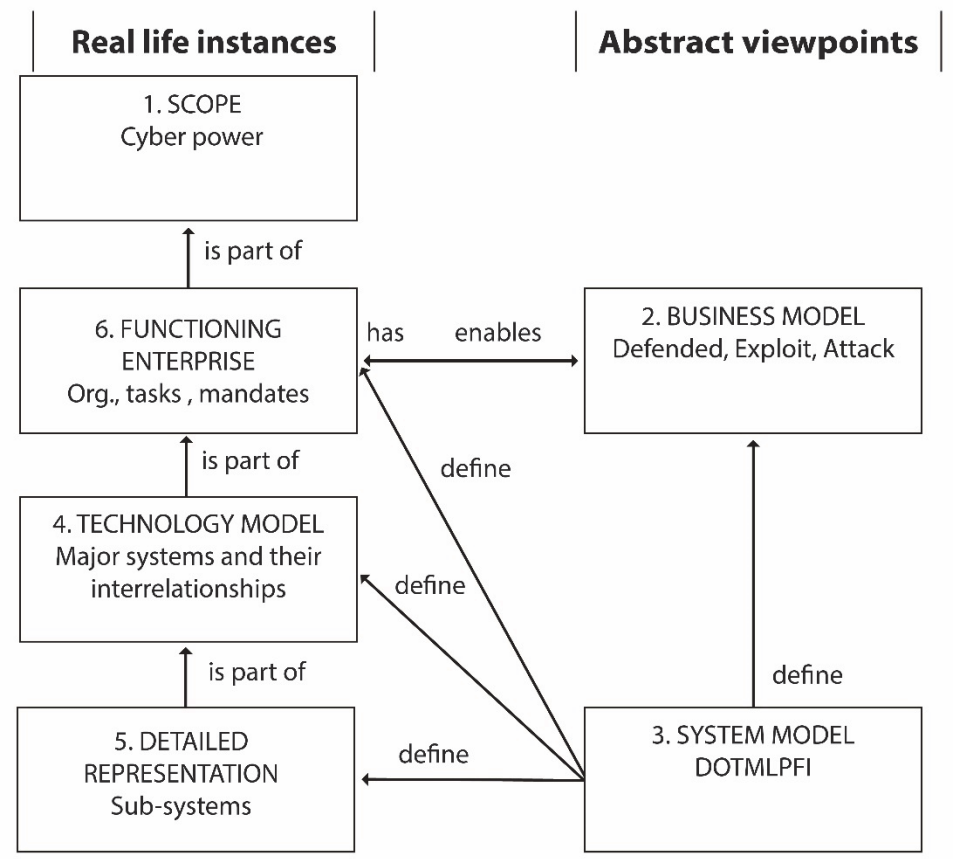


Figure 1. The CCMM viewpoints arranged into real life and abstract instances (Koivisto and Tuukkanen, 2017).

Again, we note that the Russian initiatives could well be analysed through the CCMM, but in the absence of resources we have to seek simpler and more cost effective ways for initial analysis and to provide justification for potential later expansion of such research efforts. Which leads us to the notion of cyber resilience that is relatively well understood within the cyber communities of interest and is in many ways considered a central notion. Cyber resilience refers to (Björck et al., 2015)

"The ability to continuously deliver the intended outcome despite adverse cyber events".

Björck et al. (2015) consider cyber resilience at six different levels: 1) technical; 2) functional; 3) organizational; 4) regional; 5) national; and 6) supranational. For cyber resilience to be effective and efficient it needs to be addressed holistically and on several levels and in parallel. We aim to use these levels as a framework when evaluating the cyber resilience of structurally and technologically different networks.

It is evident that resilience is constructed differently in systems based on open networks compared to closed national networks. In the closed national networks resilience may be constructed by controlling and restricting information flows therein. The sought-after resilience can be achieved by controlling and protecting the information infrastructure nationally and by controlling core routers nationally. In the open network the critical infrastructure is controlled and protected by applying other means, the infrastructure may be decentralized and it may be controlled by standards and audits. Modelling the critical infrastructure of a closed national network has just begun (Nikkarila et al. 2018). In open networks, it is not generally possible or even desired to monitor and control information flows nationally. The service providers both in the critical infrastructure and routing are private companies.

3 Two-Sided[4] Wargame on Cyber Resilience

In two-sided wargaming there are two or more opposing teams of players that execute cyber operations on a map or board based playing surface

[4] "Number of Sides: The number of sides in a game is determined by the nature of the conflict and the nature of the opposition being gamed and the number of independent entities who can make decisions and take independent action that influence the direction of the game. Games can have 1 side, 1 ½ sides, 2 sides or more. The number of sides

regulated by a set of game controllers (White Cell). The control team does not assist or advise the competing teams in any way. The control team ensures that the actions taken are consistent and determine the outcomes of actions. The competing teams deploy and manoeuvre counters on the map or board in an attempt to achieve their objectives.

In this research we propose to use the format of a table top exercise (TTX[5]) to extract the desired information on the resilience of closed national network. In practice, the goal of the table top exercise for participants is to gain a greater understanding of commonalities and differences in approach and capabilities in dealing with the cyber resilience of a closed national network. The gameplay is represented on a physical map or board by using counters that represent personnel, equipment, assets and actions. The table top exercise uses matrix gaming methodology, which relies on the use of structured argumentation. Actions are proposed and argued for by the player teams in turn and a game controller determines outcomes based on the strength of supporting and opposing arguments. A stochastic method (rolling of dice) can used to reflect the chance involved in actions if desired. The matrix gaming methodology is limited only by the players' imagination.

4 Framing the Two-Sided Cyber Wargame on Cyber Resilience

The idea of the wargame (experiment) is to reveal the new properties that a closed national network brings when securing individual systems. It is likely that the establishment of a closed national network causes effects e.g. situation awareness, and one object of the experiment is to unveil these effects as well. Essentially we propose to experiment on the changed circumstances with different new technologies, strategies or tactics, as wells as procedures (TTPs) compared to more traditional ones. This approach is used for development of TTPs not yet connected to any real cyber operation.

---

does not always equal the number of cells." Simpson, William L. Jr: https://www.movesinstitute.org/wp-content/uploads/2017/09/WargamingTerms.pdf

[5] Simulation wargames depicting an armed conflict.
• A table-top exercise is a discussion-based wargame where players sit at tables and interact with one another to address the key issues of the wargame. While not specifically structured as a turn based game, facilitators will often cause players to consider issues in a particular order, to determine the relationship between specific decisions or actions. Simpson, William L. Jr: https://www.movesinstitute.org/wp-content/uploads/2017/09/WargamingTerms.pdf

At the technical and tactical level we are considering the two paradigms:

1. open source software, open architectures, industry best practices (hardening of operating systems, configuring of open security products), solid commercial third party products, ability to fix open source components, and
2. Security by obscurity, tight restrictive rulesets, strict firewalling and segmenting from the outside internet, “Running national Internet as a company intranet".

Notably, we shall consider how these differ when considering national cyber defence at the strategic and operational levels.

We propose to form a cyber wargame that uses at least one red team against at least two blue teams. In addition, there could be different evaluator teams and an umpire (White team). One of the blue teams relies on open network infrastructure and the other on closed network infrastructure. The Red team represents an outside threat and attacks (influences) both of the blue teams simultaneously. In the game we propose, the blue teams compete on the level of their network’s cyber resilience against one red team, i.e. their “ability to continuously deliver the intended outcome despite adverse cyber events” is evaluated. The tools used by the red team are equivalent to a certain extent and that enhances the comparability and validity of the exercise. Nevertheless, during the exercise the red team improves its attack methods depending on their mission success. Results are compared in order to find out the differences in cyber resilience of the network infrastructures studied.

The scope of this paper is not to present an exclusive formalism of the suggested wargame. Instead, our aim is show the need for thewargame and to present example guidelines for its design process. We propose forming representative use cases that may be applied when deriving the actual scenarios of the wargame. For example, one use case could be the usage of a cloud services provider for a company’s (or an authority’s) internal and external needs. In practice this could include email and calendar services, shared disks, intranet, and extranet just as an example. The notional company could operate in international markets either exporting or importing a significant amount of goods (or services), or the qualitative value of the goods is vital for the country in question. The services could also be immaterial such as programming. Another use case could be how the closing of the national networks affects citizens’ internet services when operating domestically and/or abroad. One could also form a use case where the core services, such as resolving the DNS-address of a foreign website from inside the closed national network, are tested. Additionally

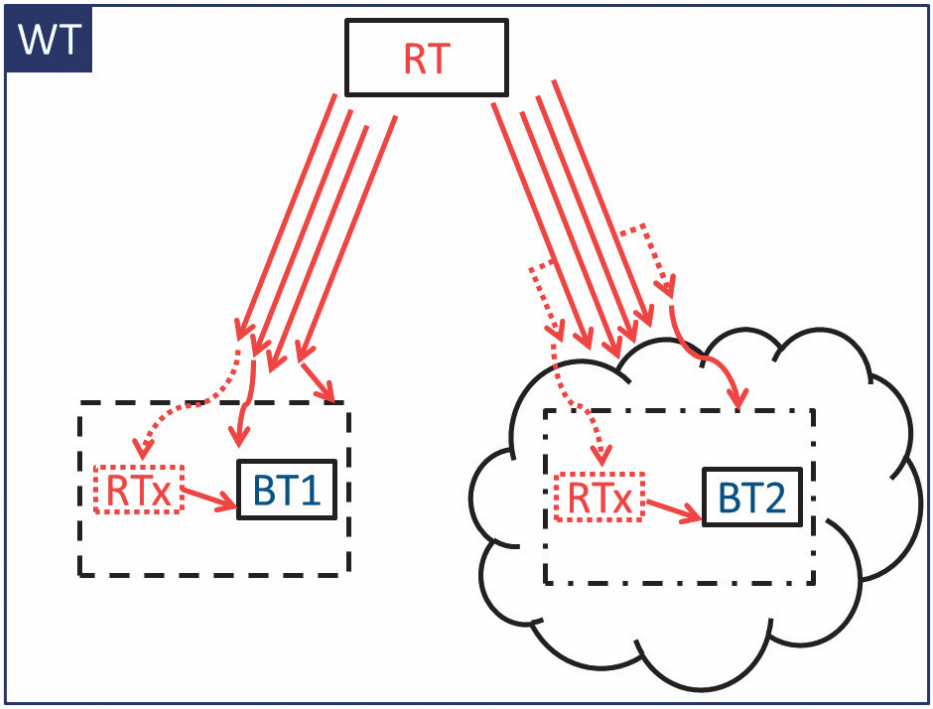


Figure 2. A schematic outline of the two-sided cyber wargame. The open network is presented on the left. Blue team 1 (BT1) relies on the open network infrastructure (dashed line box). The closed national network is presented on the right. Blue team 2 (BT2) relies on technologically different network infrastructure (dashed-dotted line box). Red team (RT) is actively attacking both blue teams and possibly operating inside both networks (RTx). The red arrows represent attack-methods and their variations. Attacks can be targeted both against the infrastructure or the specific blue team systems. The control team (White team, WT) holds all the knowledge in the game and enables all events in it. Therefore, WT is visualized as a solid line consisting of everything in the game.

one could also test how standard email services operate inwards and outwards of the closed national networks or how end-to-end encryption is affected by the closing process.

It is worth considering how the red team operates in practice as the systems are different and the goal is to extract results that are idealistically commensurate. We acknowledge that the results are not necessarily commensurate and consequently, the comparison of the two networks is not straightforward. It is also important to value of the costs related to the amendments to the closed (and open) network that the actor encounters

when it has to fix the vulnerabilities discovered from their proprietary techniques.

5 Planning and Executing the Wargame

In the planning phase, the aim is to form a representative picture of the technical structure of a closed national network. The formation of the technical framework structure of a previously unknown or significantly different network requires a substantial amount of research and expertise. Ideally, a multinational group of experts is formed to resolve how the technical functionality of a closed network differs from the functionality of the open network. Furthermore, the most important infrastructure assets (e.g. internet core routing techniques)[6] of the studied networks need to be defined for example in the form of use cases. These assets contribute to the technical framework that forms the 'game board' and influences the rules of the wargame.

In the following step of the planning phase the rules of the wargame are defined. These rules include, for instance, what kinds of systems are to be protected by B1 and B2; at which level of cyber resilience these systems are located; what kinds of outcomes the determined systems need to deliver. To quantitatively compare the cyber resilience of different networks, measures of effectiveness (MoEs) need to be defined and the scoring principles need to be included in the rules.

For the wargame to be playable and beneficial there need to be certain rules of engagement. The rules of engagement both enable and restrict the RT actions in an appropriate manner. For instance, in a traditional technical level cyber wargame an initial compromise is guaranteed at the beginning to ensure the playability of the game. In the proposed wargame, it has to be decided whether the initial access is guaranteed or if the game is to be played by applying alternative means. The objectives and means of the RT are defined and phased. Phasing enables a profounder analysis of the cyber resilience of the different networks. (What factors do we want to compare in the two networks?)

The overall purpose of the wargame is to unveil the differences in the cyber resilience of a closed national network and the open network. Consequently, all other elements (e.g. RT attacks, BT systems and their operating principles) are standardized if and when possible and relevant.

[6] E.g. ENISA's Threat landscape and good practice guide for Internet Infrastructure

The authors realize that to construct this wargame on a technical level is extremely challenging. Therefore, at the beginning we propose to apply table top wargaming. The table top wargame workflow could be for example as described in the following. A question set has to be formed i.e. the specific questions we want to answer with wargaming. Also the MoEs, assumptions, abstractions and rough scenario setting need to be formed. In the proposed case BT1, BT2 networks have to be defined as well the networks in which they are encapsulated. In the following phase the wargame rules need to be defined.

Since we are comparing two alternatives, it is vital for the success of the study to ensure commensurability or, if the results are not commensurate by nature, to recognize their noncommensurability. The technical and structural differences between BT1 and BT2 networks need to be described in sufficient detail by subject matter experts (SMEs), especially those factors that are expected to influence the MoEs.
– A Rule of thumb: things that are to be compared, are to be conducted in detail, the rest with less detail.
At the same time, one has to consider the RT's capabilities and possibilities for action.

All assumptions, abstractions, MoE and other background information need to be documented (a version-controlled living document).

6 Conclusions

In this article, we have reviewed several potential analytical frameworks and as an intermediate conclusion we propose to set up a table top cyber wargame that tries to find resilience differences between closed national networks and open networks. The proposed cyber wargame brings more authentic, yet simulated, information of the operational properties of structurally and technologically different networks. It is important to note that designing, constructing and executing the proposed wargame requires a substantial amount of expertise from technical up to strategic levels. Consequently, the authors suggest that a multinational team is formed to respond to the challenge. This paper serves as an intermediate step in the continuation towards more detailed research that is necessary to understand how the formation of closed national networks affects cyberspace. The authors acknowledge that the work is at the beginning and the situation is constantly changing. However, this research improves situation awareness and gives potential directions to direct resources.

Acknowledgement

The authors wish to thank Capt Juha Kukkola (Finnish National Defence University) for his valuable comments and opinions during the writing of this article.

References

Anteroinen, J., 2012: Integration of existing military capability models into the comprehensive capability meta-model, *IEEE International Systems Conference (SysCon), 2012 IEEE*.

Björck, F., Henkel, M., Stirna, J., and Zdravkovic, J., 2015: Cyber Resilience – Fundaments for a Definition. In *New Contributions in Information Systems and Technologies*, Rocha, Á., Correia, A.M., Costanzo, S., and Reis, L.P. (Eds.), pp. 311-316.

Choucri, N., Cyberpolitics in International Relations, Cambridge: *MIT Press*, 2012, pp. 221-238).

Kantyshev, P., and Golits'na, A. (2016) "Runet budet polnost'iu obosoblen k 2020 godu", *Vedomosti, 13 May*.

Klimburg, A., 2012: National Cyber Security Framework Manual, *NATO CCD COE Publication, Tallinn 2012*.

Koivisto, J. and Tuukkanen, T., 2017: Comprehensive capability meta model tested by a cognitive radio, *Military Communications Conference (MILCOM), IEEE*.

Kuehl, D., 2009: From Cyberspace to Cyberpower: Defining the Problem, in Kramer, F., Stuart, S., and Wentz, L. eds. (2009), *Cyberpower and National Security*, Washington, D.C.: National Defense University Press.

Kukkola, J., 2018: The Russian Segment of Internet as a Resilent Battlefield. *ISMS Annual Conference 2018*, *"Military Sciences and Future Security Challenges" (ISMS), Warsaw Poland*

Kukkola, J., Nikkarila, J-P and Ristolainen, M., 2017a, Shaping Cyberspace –A predictive analysis of adversarial cyber capabilities, *IST-145 specialists' Meeting Predictive Analytics and Analysis in the Cyber Domain, Sibiu, Romania*

Kukkola, J, Ristolainen, M. and Nikkarila, J-P, 2017b: Game Changer: Structural Transformation of Cyberspace, Riihimäki: *Finnish Defence Research Agency*. [Online]. Available: http://puolustusvoimat.fi/web/tutkimus/tutkimuslaitoksen-julkaisut [Accessed 14 May 2018].

Nikkarila, J-P, Åkesson, B., Kuikka, V., and Hämäläinen, J., 2018: Modelling Closed National Networks – Effects in Cyber Operation Capabilities, *17th European Conference on Cyber Warfare and Security (ECCWS), Oslo, Norway.*

Nye, J., 2010: Cyber Power, Cambridge MA: *Belfer Center for Science and International affairs, May 2010*.

Simpson, W. L. Jr: https://www.movesinstitute.org/wp-content/uploads/2017/09/WargamingTerms.pdf

JOINING FORCES

Epilogue

Margarita Jaitner
Teodor Sommestad

For the past decade or so, Russia has set aim to reemerge as a global power, able to shape the global order in many domains. This includes cyberspace, where Russia is currently not a global power in terms of commercial activity. The world's four largest companies in terms of market value are all American information technology enterprises (Apple, Google, Microsoft, and Amazon). Their software typically runs on hardware produced in China. China is also home to the information technology companies Alibaba and Tencent, which make the world's top-ten list in terms of market value. Yandex, Russia's largest information technology company is used more often for internet searches in Russia than Google is. In addition, Russia has its own services for social networks, email etc. However, Yandex is worth less than 2% of Google and, globally, Yandex provides less than 1% of the internet searches Google provides[7]. As mentioned in Chapter 1 of this anthology, Russia has acknowledged this relative weakness and wishes to change the status quo by reshaping international agreements, take advantage of vulnerabilities of more developed nation states, and protect itself in cyberspace.

Together with the previous anthology on this topic, "Game Changer", the collection of articles in this anthology provides a comprehensive account of the goals set and the means envisioned by Russia. As such, these two anthologies are essential for anyone seeking an insight into how Russia understands the concepts surrounding cyberspace, be it the concept of information war or struggle, coexistence, or cooperation in cyberspace. The two anthologies also present a thorough account of how any defensive or offensive-minded actor may want to pursue activities aimed at shaping the global cyberspace. Going beyond mere understanding, the actual volume also presents valuable considerations to be made when encountering Russia's conduct in cyberspace. In short, this anthology should be of great interest to researchers, policymakers as well as military professionals concerned with Russian efforts in cyberspace.

---

[7] According to StatCounter Google provided 92% of all internet searches in December 2018, while Yandex provided 0.5%. [Online] Available at: http://gs.statcounter.com/search-engine-market-share

Following these developments is of great importance, not the least for the Swedish Defence Research Agency, FOI. Our researchers continuously conduct research in order to understand Russian ideas regarding cyberspace and its actions within it. For example, Ulrik Franke has made an effort to analyze Russia's information warfare by studying official Russian government documents[8]. Therefore, we are grateful for the invitation to contribute to the current anthology, and we are looking forward to further opportunities to cooperate even closer in our future research efforts. In this epilogue, there are suggestions of research topics that could be addressed in such cooperation projects.

1 Russian aims and the implementation of RuNet

As noted by the authors, Russia plans to reduce its dependence on the outside world, e.g., by reducing the amount of domestic traffic that is routed across the geographical border to 10%. However, it would be unwise to assume that Russia is aiming for total isolation. Neither the statements made by the Russian leadership, the official policies, nor the power projection, regionally or internationally, support such a hypothesis. In addition, President Vladimir Putin has repeatedly called for international cybersecurity cooperation[9] and Russia has repeatedly made efforts to introduce international norms of conduct in information space[10] (which is the preferred term in Russia), while at the same time developing policies for a "digitally sovereign RuNet". Therefore, it can be speculated that Russia does not only seek to define and build a national segment of the internet, but also to promote norms and standards that would apply globally, thus shaping the international cyberspace. Chapter 4 describes

---

[8] Ulrik Franke, War by non-military means – Understanding Russian information warfare, FOI-R--4065—SE, 2015.

[9] For example: RIA Novosti, "RF hochet prodvigat' svoi initsiativy po kiberbezopasnosti na ploshhadke OON," (2018, Jul 06) [Online] Available at: https://ria.ru/20180706/1524089582.html

[10] For example: International code of conduct for information security, Annex to the letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359), (2011). Further, Russia is an active part of the Working Group on the Long-term Sustainability of the Outer Space and has made particular efforts to introduce guidelines within the UN COUPOUS Guidelines on the Long-term Sustainability of Outer Space Activities. Efforts to establish norms are also noted in Chapter 3, as well as in the previous volume. For a more detailed insight into Russian normative efforts on the international arena, and why these are problematic, see Vendil Pallin, Carolina, "Russian Information Security and Warfare Strategy" in: Kanet, Roger E. (ed), "Routledge Handbook of Russian Security" (2019, in print), Routhledge.

this as something Russia may perceive as a successful scenario. This opens up for a set of interesting questions regarding Russia's approach to establishing such norms. Indeed, there is potential for further fragmentation of cyberspace through states adhering to Russian ideas and following Russia's suit. For example, Kazakhstan and Uzbekistan are already implementing SORM systems to monitor networks.[11] On the other hand, it is likely that various organizations and states who oppose fragmentation will react to the changing characteristics of cyberspace. The similarities and differences between Russia's and other nations' aims, as well as the tradeoffs each nation may be prepared to make, should be studied further.

At this point, it is important to remember Russia's particular terminology. As noted in many places in this anthology, the term "cyber" does not enjoy the same popularity in Russia as it does in the Western Hemisphere. Instead, official documents use the term "information". This, in turn, reflects the wider meaning of the term, where "information warfare" includes both what in western terminology is commonly referred to as cyber warfare, and information (psychological, or influence) operations. Through this lens, a conflict in cyberspace becomes a struggle for control of information flows[12]. In the words of Thomas Rid: "Cyber security has a broader meaning in non-democracies: For them, the worst-case scenario is not collapsing power plants, but collapsing political power."[13] Hence, Russia probably does not only desire to patrol the space it regards at its own for malicious code, but also for undesirable ideas. This can have an impact on how the notion of "'digital sovereignty" can be interpreted as well as what kind of actions Russia might want to continue to be able to carry out, and where. In this context, the notion of the "Russian world", repeatedly used by the Russian leadership[14], can be an important factor. If a "digitally sovereign" RuNet is supposed to be a Russian safe haven, how do individuals who identify themselves as Russians, but reside outside Russia, or Russia's allies reach this safe haven? In addition, how does Russia want

---

[11] Predsedatel' Komiteta natsional'noi bezopasnosti Respubliki Kazakhstan, Prikaz ot 20 dekabria 2016 goda No. 91, "Ob utverzhdenii tehnicheskogo reglamenta "Obshhie trebovanija k telekommunikatsionnomu oborudovaniiu po obespecheniiu provedeniia operativno-rosysknyh meropriiatii, sbora i hraneniia sluzhebnoi informatsii ob abonentah," (2016, Dec 20) [Online] Available at: https://online.zakon.kz/Document/?doc_id=39110433

[12] Denning, Dorothy E., "Power over Information Flow." (2009).

[13] Rid, Thomas, "Think Again: Cyberwar", Foreign Policy, (2012, Feb 27) [Online] Available at: https://foreignpolicy.com/2012/02/27/think-again-cyberwar/

[14] For example: Pravda.ru, "Putin budet zasshishhat' russkii mir vsei moshh'iu," Pravda.ru, (2018, Nov 03), [Online] Available at: https://www.pravda.ru/news/politics/authority/31-10-2018/1398064-0/

to continue to promote its ideas in the global information space? Ultimately, it appears as if Russia is attempting to build a fort, but not without the necessary crenels.

The authors of this anthology present an extensive account of official communication and policies postulating the creation and safeguarding of a sovereign and delimited space within Russia's "digital borders". However, cyberspace develops rapidly, and not in a vacuum. It is influenced by other actors than Russia and its allies as well as the rules of national or global economy. Therefore, it is necessary to carry out regular reality checks of the concepts and ideas presented in this anthology, as well as their implementation. Large parts of the implementation will remain clandestine and therefore only intelligence services may be able to provide a definitive status on many of the implementations. At the same time, the described policies include extensive requirements that apply to privately held entities, in particular foreign actors within cyberspace. It is our belief that researchers who solely rely on open source material still can assess the level of success of the implementation to some extent. For instance, it is noted in Chapter 2 that the public-private-partnership effort related to the surveillance solution SORM led to "a haphazard and ineffectual implementation." In particular, the declining rule-of-law as well as corruption in Russia may be the first-hand reasons for failing plans and are something to watchful of. Even now, some openly available sources indicate problems in implementing some of the surveillance apparatus.[15] Furthermore, political communication and actual plans may differ and plans or claims may be made for political reasons, but without any ambition to realize them. Besides failed or fake plans, the exact implementation of the ideas and concepts requires some necessary assessments. For example, the type of joint exercises propagated in the policy documents mentioned in Chapter 2 might allow further estimates of the importance of following through with the cyber defense efforts and actual preparedness. In certain constellations, it might be of particular value to pinpoint the exact realities that hamper the implementation of Russian plans in information space.

[15] Kolomychenko, Maria, Lindell Dada, "Vne proslushki: pochemu Roskomnadzor i FSB sudiatsia s operatorami sviazi," RBK, (2017, Nov 09), [Online], Available at: https://www.rbc.ru/technology_and_media/09/11/2017/5a03187e9a7947d88f988f53

2 The strategic advantage of sovereignty and ability to disconnect

Both this anthology and its precursor elaborate on the advantage a state would have *if* it was able to restrict access to its own cyberspace while others nations could not restrict access to theirs. Following this train of thought, we suggest a few aspects for further study.

First, it is worth assessing under what circumstances the controls set up at the national border would make a difference in actual cyber conflicts and operations. System administrators of a typical computer network know that covert channels may be present in their network as long as any traffic is allowed through the firewall. Every system administrator also knows (or should acknowledge) that there may be malicious or compromised insiders in their network. It is hard to see why this should not apply to computer networks as large as those of an entire nation. Thus, preventing all possibilities for foreign agents to gain computer network connectivity in a large country such as Russia appears to be immensely difficult. Further assessment of the types of cyber operations that can be thwarted or better handled with an ability to connect would be interesting.

Second, the capacity to exercise power outside one's own borders goes along with the status of being a global power. Russia has developed, and continues to develop, a wide array of approaches to do so via, or with the help of, cyberspace. However, Russia's implementation of "digital sovereignty" may hamper its own ability to act in the global cyber or information space. Thus, Russia may have to balance its version of "digital sovereignty" against access to global cyberspace and their ability to exercise power elsewhere. In this context, it is also interesting to follow the Russian assessment of whether its activities indeed lead to an asymmetric advantage as well as how the results of such an assessment may change the Russian approach.

Third, it is conceivable that the development to isolate RuNet can be turned against Russia. Today, multinational companies, including those that operate in Russia, are dependent on cross border internet connections. If they are forced to prepare for a potential disconnection between RuNet and the global internet, and indeed follow these demands, the threshold for other nations to disconnect from Russia may be lowered, as the multinational companies still will be able to continue running their business without the connectivity. Thus, the capability to run a state's cyberspace autonomously may also increase the likelihood that it will have to be run

autonomously, even if this is not desired. The likelihood of such course of events could be investigated, e.g. using game theoretic models.

Fourth, the political impact may differ from the anticipations of Russia's plans. Protectionism usually comes with concessions and the exact details of these concessions will not become clear until the implementation is in place. Delimiting the part of cyberspace that Russia perceives as its own may lead to a variety of challenges, such as discontinuation of services by foreign companies and limited abilities for Russia-based companies to operate elsewhere. As a result, Russia may lose businesslinks to what Russia defines as its legitimate zone of interest. A valid question in this context is how Russia would handle such a course of events, in particular, whether Russia would be tempted to resolve the situation, and by what means.

Fifth, the economic consequences of a contingency plan that involves disconnecting from the global internet could be assessed and put into relation with other potential defense investments. Policies aiming for autonomy and technical solutions that implement them may hamper Russian companies in a number of ways. A better sense of the costs involved might help to predict where Russia is moving, and how fast.

3 The asymmetry to expect

Yet another issue that deserves further attention is to what extent the developments and plans related to RuNet lead to asymmetry and to what extent they may instead lead to a more symmetric status quo. As observant readers may have noticed, many of the mentioned developments are by no means unique to Russia. For example, governmental monitoring of internet connections and regulations concerning where private data can be stored are present in other nations too. It is possible, perhaps even likely, that the Russian implementations and motives differ from those of other nation states, even when they appear similar up front. Comparisons of policy developments in Russia to those in other nation states would be interesting. Such comparisons would increase the understanding of the asymmetry that should be expected.

Another issue is that the notion of "digital asymmetry" may become more faceted than previously assumed and pertain to other things than RuNet. As described in this anthology, Russia views the informational and the cyber aspect as one, whereas its potential rivals address the concepts individually. The different approaches towards cyberspace in itself can bring about a

certain asymmetry. Russia's rivals may focus on either cyberspace or information control and neglect the other or the lack of coordination between the two aspects. Meanwhile, Russia may be an actor that successfully integrates the approaches, thereby gaining relative advantages. In general, Russia's centralization of efforts related to cyber and information may lead to further asymmetries in terms of priorities, behavior, and technologies.

In addition to the developments related to RuNet, the rapid development of the technology that surrounds and impacts cyberspace presents researchers with yet another question: How do new technologies influence the way Russia perceives and desires to utilize cyberspace? For example, the advances within the field of Artificial Intelligence (AI) may have a profound impact on how Russia perceives and attempts to deal with the global cyberspace and maybe even its definition of "digital sovereignty". AI might present Russia with an opportunity to define its digital borders in a flexible manner, reflecting prevailing opinions and loyalty, rather than geographic location. President Putin recently suggested that the nation that leads in AI "will be the ruler of the world"[16] and a national AI development roadmap is currently underway[17], which indicates the idea that this area may be transformational. The development and proliferation of AI may also have some other, not yet understood, impact on either Russian ideas regarding cyberspace, or their manifestation.

4 Final words

Having introduced a number of leads for further research, it should be underlined that the authors have conducted an extensive, invaluable investigation into Russian efforts and provided actionable alternatives for handling the resulting challenges. Yet, in an ever-developing area of operations, there will always be new aspects to investigate and new circumstances to take into consideration. As the changing global cyberspace can be shaped by and is shaping the Russian approach to cyber, we look forward to cooperating with the authors in future research projects.

---

[16] TASS, "Putin: lider po sozdaniiu iskusstvennogo intellektastanet vlastelinom mira," TASS, (2018, Sep 01), [Online], Available at: https://tass.ru/obschestvo/4524746

[17] TASS, "Dorozhnaia karta razvitiia iskustvennogo intellekta v Rossii poiavitsia k seredine 2019 goda," TASS, (2018, Okt 17), [Online], Available at https://tass.ru/ekonomika/5687237

POST SCRIPTUM – Where is the ball now?

Juha Kukkola

Post Scriptum was added to this collection only a couple of days before it was sent to print. Our team of researchers had been following a new legislative drafting process in the Russian duma when editing this collection and decided that it needs to be included as well. What follows is a brief description of a law draft concerning the procedure and responsibilities of disconnecting the Russian segment of the Internet from the global Internet. It is part of the implementation of the national program of Digital Economy that has been discussed in many of the articles of this collection. Additionally, some reflections on the developments concerning the Program itself are included in the end of this analysis.

A law draft amending the Federal law on communications (*O Sviazi*) was submitted by two members of the Federal Council, A. A. Klishas and L. P. Bokova, and a duma representative A. K. Lugovoi in December 14, 2018.[18] A. A. Klishas is by education and background a lawyer and has a PhD in law and has written, among other things, about state sovereignty. L. P. Bokova is a teacher by education and sits in the Interim Commission of the Council of the Federation to protect state sovereignty and prevent interference in the internal affairs of the Russian Federation.[19] A. K. Lugovoi is an ex-KGB agent and a Federal Security Services (FSO) official and has been accused of poisoning and killing the Russian ex-spy

[18] *Federal'nyi zakon [proekt] "O vnesenii izmenennii v nekotorye zakonodatel'nye akty Rossiiskoi Federatsii"* [Federal law [project] "On Amendments to Certain Legislative Acts of the Russian Federation"], No. 608767-7, 14.12.2018 [online]. Available: http://asozd2c.duma.gov.ru/addwork/scans.nsf/ID/E794ACF3791E3C7B43258363004AC230/$FILE/608767-7_14122018_0138233894-1.pdf?OpenElement [Accessed: 19th December 2018].

[19] *Postanovlenie Soveta Federatsii Federal'nogo Sobraniia Rossiiskoi Federatsii "O sozdanii Vremennoi komissii Soveta Federatsii po zachshite gosudartsvennovo suvereniteta i predotvrachsheniiu vmeshatel'stva vo vnutrennie dela Rossiiskoi Federatsii", 14 iiunia 2017 goda No. 172-SF* [The degree of the Federal Council of the Federal Assembly of the Russian Federation "On the establishment of the Interim Commission of the Council of the Federation to protect state sovereignty and to prevent interference in the internal affairs of the Russian Federation"] [online]. Available: http://council.gov.ru/activity/documents/81373/ [Accessed: 19th December 2018].

Aleksandr Litvinenko in London in October 2006.[20] Klishas and Bokova are members of the United Russia party and Lugovoi is a representative of the Liberal Democratic Party of Russia.

In the explanatory note of the law draft, the submitters claim that the law is intended to protect Russia against United States' openly declared aggression. As a proof of their argument, they refer to the 2018 National Cyber Strategy of the United States of America.[21] The law draft is aimed at ensuring the safe and sustainable operation of the information and telecommunications network called Internet in the Russian Federation. It is intended to create the legal basis for the enabling of the routing of Internet traffic inside Russian physical borders, the controlling and managing in a centralized way cross-border data traffic, the installing of equipment to restrict and close traffic inside Russian networks, the creating of infrastructure to secure the functioning of the Russian Internet if it is disconnected from the outside, and the enabling of mandatory cyber exercises to train the maintaining of the functionality of the Russian segment of Internet under threat. The law draft designates the centralized control and executive authority of the system it proposes to the Russian government. It is important to note that the law does not demand the disconnection of the Russian segment of Internet from the global Internet if there is no threat to its integrity, resilience and security.

The main points of the law draft in more detail are the following:

1. Operators[22] must report practically all information about their networks including physical connections crossing Russian Federation's borders, Autonomous System numbers, IP-address spaces, DNS-systems, network architecture, and routing tables to the *Rozkomnadzor*[23]. Operators are required to ensure the

[20] Personal information is based on https://ru.wikipedia.org [Accessed: 19th December 2018].
[21] The President of the United States. *The National Cyber Strategy of the United States of America,* September 2018 [online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [Accessed: 19th December 2018].
[22] Operator is used here as a shorthand for the Internet service providers (ISP), the holders and operators of anonymous system (AS) numbers (large groups of IP addresses with a single routing policy), the operators of Internet traffic exchange points (IXPs), and the telecommunication companies etc. operating cross-border (that cross Russian state border) communication networks and connections
[23] *Rozkomnadzor* i.e. the Federal Service for Supervision of Communications, Information Technology and Mass Media is "responsible for monitoring and supervising the mass media, including electronic and mass communications, information

Rozkomnadzor to have the access to their networks and must allow the installation of monitoring equipment into their networks. Operators must manage their Internet routing in accordance with the demands of the *Rozkomnadzor* and they must secure their connections to other operators. This includes abstaining from connecting their networks to networks of such operators who do not follow the requirements stated in the law draft. These demands do not limit the requirements to cooperate with the investigative authorities and security services as stated in other laws etc.

2. *Rozkomnadzor* must keep a register of the information declared by the operators and confirm that they are acting in accordance of the requirements of the law draft. It has the right to request additional information from the operators.

3. To manage threats to the resiliency, security and integrity of the Internet and common telecommunication networks the *Rozkomnadzor* is allowed to monitor the networks of operators to detect threats; it is allowed to perform centralized network management to eliminate threats; and it is obliged to provide the operators the technical equipment to counter threats the installation of which is handled by a specifically authorized executive authority. Accordingly, the centralized management of the networks is conducted through the above mentioned equipment or through binding instructions. Moreover, the *Rozkomnadzor* is responsible of informing operators of imminent threats.

4. The executive authority responsible of the organizational, administrational and technical tasks stated in the law draft is the Radio frequency service (*radiochastotnaia sluzhba*) which is part of the *Rozkomnadzor*.[24]

---

technologies and communications, and control and supervision of the compliance of the processing of personal data with the requirements of the legislation of the Russian Federation in the field of personal data, as well as the functions of organizing radio frequency service." (*Polozhenie Pravitel'stva Rossiiskoi Federatsii "O Federal'noi sluzhbe po nadzoru v sfere sviazi, informatsionnykh tekhnologii i massovykh kommunikatsii"* [The Degree of the Russian Government "On the Federal Service for Supervision in the Sphere of Communications, Information Technologies and Mass Communications] ot 16 marta 2009 g. [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_85889/ef9df1275694e64fea6b1b2a6140b7852e87827a/ [Accessed: 13th February 2019]).

[24] *Polozhenie Pravitel'stva Rossiiskoi Federatsii "O radiochastotnoi sluzhbe"* [The Degree of the Russian Government "On radio frequency service"] ot 14 maia 2014 g. N

5. Exercises must be conducted to ensure the security, integrity, and resiliency of the common telecommunication network of the Russian Federation.

6. The equipment of the central management of the Russian segment must reside on the Russian territory and the operators of state information systems should not be allowed to use data bases and technological equipment residing outside Russian territory to manage those systems.

7. A national system of domain name servers and resolvers is to be created. *Rozkomnadzor* is responsible of this and operators must use software that ensures the utilization of the demands set by *Rozkomnadzor* (i.e. they must use national DNS services). Those operators operating their own DNS services must register them to Rozkomnadzor.

8. Operators are not responsible for restricting or allowing traffic if they have the above-mentioned equipment installed. These functions are the responsibility of the *Rozkomnadzor*. The functions and equipment are controlled remotely, and their management is based on IP-addresses, domain names or "other information" necessary to counter threats.

In the context of the Program of Digital Economy a few remarks can be offered about the law draft. Firstly, one of the main differences of the law draft to existing law and other competing administrative proposals is the role given to *Rozkomnadzor* instead of the security services in protecting the Russian segment of the Internet. This seems to be based on the idea that the Internet is part of the common information and telecommunication network and thus falls under civilian and political control. It also reflects the changing circumstances in the power struggle between the security services (i.e. Federal Security Service and Federal Protective Service), the Ministry of Digital Development, Communications and Mass Media of the Russian Federation (*Minkomsviaz*), the Ministry of Economic Development and the Ministry of Defence.[25] If the law draft goes through

---

434 (red. ot 25.9.2018) [Online]. Available: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102349694&rdk=&backlink=1 [Accessed: 13th February 2019].

[25] Peterson, D. J. *Russia and the Information Revolution*. Santa Monica: RANS, 2005; Ristolainen, Mari, 2017. "Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West," *Journal of Information Warfare*,

without significant changes, *Minkomsviaz* would be the winner in this round battle.

Secondly, the law explicitly states that the operators do not have to pay for the equipment required and are freed of legal responsibilities if they install the necessary equipment. This is a slight departure from previous law drafts concerning critical information infrastructure where the costs and responsibilities were designated to the private sector.[26] The push-back from the ISPs has significantly delayed these projects so this 'burden sharing approach' might be used to try to get the system working in the timeframe of the Digital Economy program i.e. by 2024.[27] At the time of writing, although the law draft has passed the first voting in the Duma and obtained wide support from the government officials and politicians, the private sector is in a characteristic way passively resisting the law.[28]

Thirdly, as commentators have already pointed out, it is unclear how the new system would be financed.[29] The federal funding for the Digital

---

16(4), pp. 113-131; Kolomychenko, Mariia. "Kiberspetsclyzhba: Sberbank predlozhil sozdat' shtab bor'by s khakerami [Cyberspecialservice. Sberbank proposed the creation of a headquarters to fight hackers]". *RBK*, 1 sentiabria 2017 [Online] Available: https://www.rbc.ru/technology_and_media/01/09/2017/59a9799f9a7947375702db15?from=center_7 [Accessed: 13th February 2019]; *Roskomsvoboda. Izoliatsiia Runeta odobrena Mintsifroi i Rockomnadzorom* [The isolation of Runet approved by Mintsifroi and Rozkomnadzor]. 17.1.2019 [Online], Available: https://roskomsvoboda.org/19830/ [Accessed: 13th February 2019]; Kolomychenko, Mariia. "Minfin dal otritsatel'nyi otziv na zakonoproekt o "suverennom Runete" [Minfin gave a negative review on the bill on "sovereign Runet"]*"*. *RBK*, 18 oktiabria 2017 [Online], Available: https://www.rbc.ru/technology_and_media/18/10/2017/59e7409d9a79475efb991b41?from=main [Accessed: 13th February 2019].

[26] *Federal'nyi zakon O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi* Federatsii [Federal law "On the security of critical information infrastructure of the Russian Federation"] ot 26.7.2017 N 187-FZ. [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_220885/. [Accessed 1 November 2017].

[27] Kodachigov, Valerii. "Zakon Iarovoi poka ne rabotaet: Dlia ego vypolneniia operatoram ne khvataet dokymentatsii. [The Iarovaia law does not yet work: Operators lack documentation for execution]". *Vedomosti*, 01 oktiabria 2018. [Online]. Available: https://www.vedomosti.ru/technology/articles/2018/10/01/782493-zakon-yarovoi [Accessed: 13th February 2019].

[28] Balenko, Evgeniia, Galimova, Natal'ia, Posypkina, Aleksandra & Balashova, Anna. "Ataka iznutri: operatory protestiruiut zakon ob ustoichivosti Runeta [Attack from the inside: the operators are testing the law on the stability of the Runet]". *RBK*, 8 fevralia 2019 [Online]. Available: https://www.rbc.ru/technology_and_media/08/02/2019/5c5c51069a7947bef4503927?from=center_16 [Accessed: 13the February 2019].

[29] Ibid.

Economy has been set at 1,1 trillion roubles for 2019-2024 with additional 0,7 trillion from the private sector.[30] Of this only approximately 27,9 billion roubles is marked for 'information security' and the costs of system proposed in the law draft could be ca. 20 billion roubles.[31] This budget must be put into its context – the federal financing for other national projects i.e. Putin's May Degree programs is 25,7 trillion roubles[32] and the new military armament program (GPV-2027) is thought be somewhere around 18-20 trillion roubles.[33] Moreover, according to the proponents of digital economy the Internet economy accounts for up to 5.1% of the Russian GDP and is growing 10-15% per year.[34] Therefore, it can argued that the financial consequences and possibilities of the law draft are significant. Moreover, the system being proposed will be based on Russian technology and services which can be considered to be part of the import substitution program of the Russian government to circumvent Western sanctions.

And fourthly, and perhaps most importantly, the law draft proposes the central control of the traffic of the Russian segment of Internet through a new system which is not SORM or GosSOPKA.[35] This system would be on the top level of the system-of-systems meant to control the Russian segment of the Internet. Together with the existing systems, the new system would create a centralized hierarchical and horizontally inclusive system. The new system could be used in different phases of confrontation in

---

[30] Iastebova, Svetlana. "Itogi-2018. Rabota s dannymi stanet odnoi iz glavnykh zadach "Tsifrovoi ekonomiki". Biudzhet vsego natsproekta sostavil 1,8 triln rublei [Results of 2018. Working with data will be one of the main objectives of the Digital Economy. The budget of the entire national project will be 1.8 trillion rubles]", *Vedomosti*, 27 dekabria 2018 [Online]. Available: https://www.vedomosti.ru/technology/articles/2018/12/27/790621-rabota [Accessed: 13th February 2019].

[31] Balenko et al. 2019.

[32] Feinberg, Anton. Pravitel'stvo opublikovalo parametry natsproektov. Glavnoe. [The government has published the parameters of the national projects. The main points.] *RBK*, 11 fevralia 2019 [Online]. Available: https://www.rbc.ru/economics/11/02/2019/5c61652d9a794777d978d345?from=center_3 [Accessed: 13th February 2019].

[33] Cooper, Julian. *Military Expenditure in the Russian Draft Federal Budget for the three years 2019 to 2021: A Research Note.* The University of Oxford – Changing Character of War Centre, 2018 [Online]. Available: http://www.ccw.ox.ac.uk/blog/2018/10/19/russian-military-expenditure-by-julian-cooper [Accessed: 13th February 2019].

[34] *RAEK. "Runet podvel itogi goda"* [Runet summed up the year] 13 dekabria 2018 [Online]. Available: https://raec.ru/live/raec-news/10766/ [Accessed: 13th February 2019].

[35] cf. Kukkola, Juha, 2018. Civilian and military information infrastructure and the control of the Russian segment of Internet. *ICMCIS 2018*, Warsaw 22.-23. May 2018.

international relations, to secure flexible monitoring and controlling of the national networks. Furthermore, it could be also used to ensure their resilience and survivability even in a fragmented form, and thus enable military and political command and control over the Russian society, economy and military. The system is designed both to secure the critical infrastructure and services under an outside threat and to ensure political control of the society in the case of internal troubles. It is also meant to ensure the digital sovereignty of the Russian Federation by enabling the control of the territorial borders of the Russian Federation in the Internet and by strengthening the technological and economic base of Russian state power.[36]

Up until now, the international and Russian media has taken a cautious and sceptic approach to the program of Digital Economy and related Russian policies. As was argued in the first pages of this book it is time to take this issue seriously. The whole project of controlling the Russian segment of the Internet is based on old Soviet cybernetic ideas about network and computer enabled centrally managed society and economy in the framework of great power competition.[37] If we do not keep our eyes and ears (and mouths) open, we might someday find ourselves neighbouring a new Soviet Union, this time a digital one.

[36] cf. Kukkola, Juha, 2018. The Russian Segment of Internet as a Resilient Battlefield. *ISMS 2018*, Warsaw, 18.-19. October 2018.

[37] Kukkola, Juha. *Cyber power as means of Russian military strategy*. Doctoral dissertation [Forthcoming 2020]. Helsinki: National Defence University.

Puolustusvoimien tutkimuslaitos

Ylöjärven toimipiste
Esikunta, asetekniikkaosasto, räjähde- ja suojelutekniikkaosasto
PL 5, 34111 Lakiala

Riihimäen toimipiste
Doktriiniosasto, informaatiotekniikkaosasto, tutkimussuunnitteluyksikkö
PL 10, 11311 Riihimäki

Tuusulan toimipiste
Toimintakykyosasto
PL 5, 04401 Järvenpää

Puh. 0299 800

puolustusvoimat.fi > Tietoa meistä > Tutkimuslaitos

ISBN 978-951-25-3066-3 (painettu)
ISBN 978-951-25-3067-0 (verkkojulkaisu)
ISSN 2342-3129 (painettu)
ISSN 2342-3137 (verkkojulkaisu)