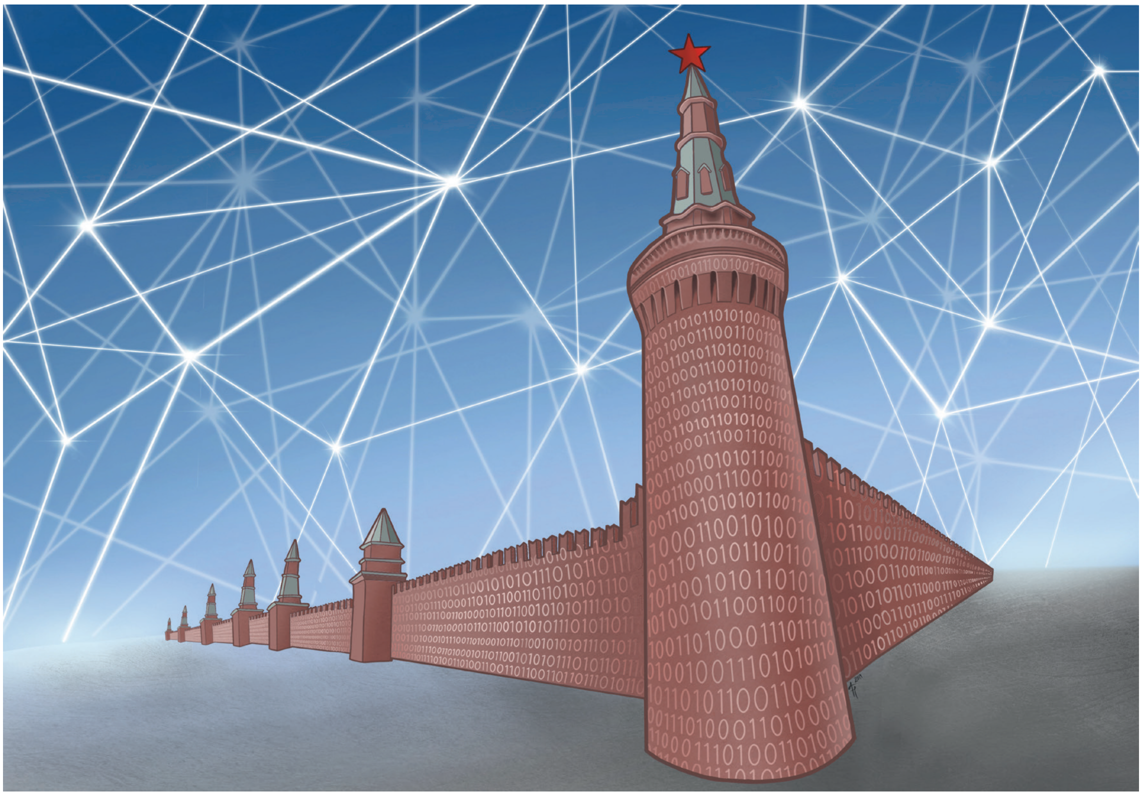
JYU DISSERTATIONS 122

Martti J. Kari

Russian Strategic Culture in Cyberspace

Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats



UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION
TECHNOLOGY

JYU DISSERTATIONS 122

Martti J. Kari

Russian Strategic Culture in Cyberspace

Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Agora-rakennuksen Martti Ahtisaari -salissa
lokakuun 11. päivänä 2019 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, Auditorium 1, on October 11, 2019 at 12 o'clock noon.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2019

Editors
Marja-Leena Rantalainen
Faculty of Information Technology, University of Jyväskylä
Timo Hautala
Open Science Centre, University of Jyväskylä

Cover illustration: Anna Hannola

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-7837-2

ISBN 978-951-39-7837-2 (PDF)
URN:ISBN:978-951-39-7837-2
ISSN 2489-9003

ABSTRACT

Kari, Martti J
Russian Strategic Culture in Cyberspace: Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats
Jyväskylä: University of Jyväskylä, 2019, 118 p. (+ included articles)
(JYU Dissertations,)
ISSN 2489-9003)
ISBN 978-951-39-7837-2

A limited amount of information has been published about the cyber threat scenarios of the Russian Federation. However, official Russian documents contain enough information to build a description of the Russian cyber threat picture. This thesis, consisting of six interconnected articles, discusses the Russian perception of cyber threats and the country's response to these threats. The data consist of 140 official Russian documents, including strategies, information security and military doctrines, draft legislation and laws.

Grounded theory is used to guide the data collection and to code the data as well as to construct a model of Russian cyber threat perception. Then the theory of strategic culture is used to explain and interpret this model. The theory of strategic culture consists of basic assumptions about the strategic environment, including threat perception, as well as assumptions about the options to respond to the threats. The theory of strategic culture identifies the factors that influence the formulation and outcome of a state's strategic culture. These factors may encompass historical, geographical, technological or political factors. The Russian cyber threat assessment reflects tensions in the international situation.

One of the underlying assumptions axioms of Russian history is that the Soviet Union was a besieged fortress, surrounded by enemies and under constant threat of attack from the West. This narrative is present in the Russian cyber threat perception just as it is part of the country's general threat assessment. To protect itself, Russia is preparing to isolate the Russian segment of the Internet from the global Internet and improving the protection of its critical information infrastructure. As a further protective measure but also as a means monitor the opposition, Russia has increased surveillance of the Internet and banned user anonymity. Russia is making an effort to replace imported information and communication technology with Russian production.

As an augmentation to previous research, this thesis, by using the theory of strategic culture, explains the long-term motives and reasons of Russia´s behaviour in cyberspace. This thesis estimates that the besieged fortress narrative guides Russia´s state behaviour in cyberspace also in future.

Keywords: Russian strategic culture, cyber threat, Russian segment of the Internet, critical information infrastructure

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Kari, Martti J
Venäjän strateginen kulttuuri kyberympäristössä: Strategisen kulttuurin teoria – keino selittää Venäjän kyberuhkakuvia ja kyberuhkan torjuntaa
Jyväskylä: University of Jyväskylä, 2019, 118 p (+ artikkelit).
(JYU Dissertations
ISSN 2489-9003)
ISBN 978-951-39-7837-2

Venäjän Federaation kyberuhkakuvista on julkaistu vain vähän tietoja. Venäläiset viralliset asiakirjat sisältävät kuitenkin riittävästi tietoja, jotta niiden avulla voidaan muodostaa kuva Venäjän kokemasta kyberuhkasta. Tässä väitöskirjassa, joka koostuu kuudesta toisiinsa liittyvästä artikkelista, käsitellään Venäjän kyberuhkakuvaa ja sitä, miten Venäjä tähän kyberuhkaan vastaa. Tutkimuksen lähteenä on ollut 140 venäläistä virallista asiakirjaa, kuten strategiat, informaatioturvallisuuden ja sotilasdoktriinit, lait ja lakiluonnokset.

Grounded Theorya on käytetty ohjaamaan datan keräystä ja koodaamista ja sen avulla on rakennettu malli Venäjän kyberuhkakuvasta. Tätä mallia selitetään strategisen kulttuurin teorialla. Strateginen kulttuuri tarkoittaa tietyssä valtiossa vallalla olevia näkemyksiä sodan ja kriisin luonteesta, maahan kohdistuvasta uhkasta ja uhan aiheuttajista sekä toiminnallisista vaihtoehdoista vastata kyseiseen uhkaan. Venäjän strategiseen kulttuuriin vaikuttaa erityisesti historia, mutta myös maantiede, teknologia ja valtion poliittinen kulttuuri ja johdon asenteet.

Yksi Venäjän historian perusoletuksista on, että Neuvostoliitto oli vihollisten ympäröimä, Lännen jatkuvan hyökkäysuhan alla oleva piiritetty linnake. Tämä narratiivi on myös osa Venäjän kyberuhkakuvaa. Suojellakseen itseään Venäjä valmistelee Internetin venäläisen segmentin eristämistä globaalista Internetistä ja parantaa kriittisen informaationinfrastruktuurin suojaamista. Suojautuakseen, mutta myös valvoakseen oppositiota, Venäjä on lisännyt Internetin valvontaa ja pyrkinyt kieltämään käyttäjien anonymiteetin. Länttä teknologisesti jäljessä oleva Venäjä yrittää korvata ulkomailta tuotavan informaatio- ja kommunikaatioteknologian Venäjän omalla tuotannolla.

Tämä väitöskirja selittää pitkän aikavälin motiiveja ja syitä Venäjän käyttäytymiselle kyberympäristössä strategisen kulttuurin teorian avulla. Arvio on, että niin sanottu piiritetyn linnakkeen narratiivi ohjaa Venäjän toimintaa kyberympäristössä myös tulevaisuudessa.

Keywords: Russian strategic culture, cyber threat, Russian segment of the Internet, critical information infrastructure

Author

Martti J Kari
Faculty of Information Technology
University of Jyväskylä
Finland

Supervisors

Professor Pekka Neittaanmäki
Faculty of Information Technology
University of Jyväskylä
Finland

Assistant professor Katri Pynnöniemi
National Defence University and
University of Helsinki
Finland

Professor Rauno Kuusisto
Finnish Defence Research Agency
Finland

Reviewers

Professor Matthew Warren
School of Information Technology
Deakin University
Australia

Dr. Mark Galeotti
Royal United Services Institute
United Kingdom

Opponents

Dr. Carolina Vendil Pallin
Swedish Defense Research Agency
Sweden

Dr. Matti Saarelainen
The European Centre of Excellence
for Countering Hybrid Threats
Finland

FOREWORD

Russia, its history, language, culture, politics and military have been my interest, both personal and professional, for almost forty years. Because of this interest, I chose Russian in high school, studied Russian language and literature at the University of Jyväskylä and graduated with a master's degree in Russian in 1993. Ten years ago, Russian cyber-related topics were added to my list of interests, and so I started to study cyber security in 2015, graduating with a master's degree in 2017.

The University of Jyväskylä is the only university in Finland where you can earn a master's degree in cyber security. The programme started in 2015, and this PhD thesis is the first in Finland by the holder of a master's degree in cyber security. Therefore, I would like to express enormous gratitude to the Faculty of Information Technology of the University of Jyväskylä for giving me the opportunity to work on my dissertation and to the Faculty of Humanities and Social Sciences, where I studied Russian language and literature.

I would like to thank the Finnish Defence Forces for providing me the possibility to study during my career, both Russian and cyber security. I am grateful to the Mannerheim Foundation and to the Marshal of Finland Mannerheim Foundation of Military Sciences (SMMSR) for the possibility to concentrate on my research and to work as a senior fellow in the Atlantic Council's Scowcroft Center for Strategy and Security's Cyber Statecraft Initiative in Washington D.C. in the spring of 2017.

I am indebted to many people whose help and support have been irreplaceable and invaluable for my research. First, I would like to thank my supervisors Katri Pynnöniemi, Pekka Neittaanmäki and Rauno Kuusisto. Katri kept up my pace of research, and as an expert of Russian defence-related topics gave excellent guidance and forced me to enter to the world of scientific theory, in this case the theory of strategic culture. Pekka also gave excellent guidance and Rauno supported me by cooperating on the writing of an article and by familiarizing me with academic conference procedures. I would like to thank my unofficial supervisor Martti Lehto, who has been my academic role model.

I am particularly grateful for the assistance given by my colleagues Panu Moilanen, Markus Salo, Arto Ojala and Jouni Pöyhönen in the Faculty of Information Technology. They supported me and gave valuable guidance on both the content and theoretical approach of my thesis. Special thanks belongs to Matthew Wuethrich from the University of Jyväskylä Language Services, who helped edit the language of this thesis. My goddaughter Anna Hannola also deserves thanks for drawing the cover image.

I would like to thank Siobhán and Pekka Toveri, who provided support and friendship during my research in Washington D.C. as well as Pasi Eronen, who helped me get the fellowship in the Atlantic Council's Cyber Statecraft Initiative. I am also thankful for two doctors, Timo Muhonen and Ismo Jantunen, who have kept me alive until now and hopefully in future.

Finally yet most importantly, I would like to thank my life companion, best friend and wife Niina, and my children Sonja, Tommi, Matti, Eeva and Peppi, who have always supported and encouraged me during my military and academic career. Finally, I would like to thank Obi-Wan Kenobi, our miniature poodle and a University of Jyväskylä reading dog, who forced me to periodically stop working with my thesis, exit the Russian besieged cyber fortress and take a walk in the fresh air.

Jyväskylä 4.9.2019
Martti J Kari

LIST OF FIGURES

LIST OF TABLES

CONTENTS

LIST OF INCLUDED ARTICLES

I. Kari, M., & Kuusisto, R. (2017). Russia: A Cyber Fortress Besieged. In *ECCWS 2017: Proceedings of the 16th European Conference on Cyber Warfare and Security (Dublin, 2017),* pp. 593–601. Academic Conferences International.

II. Kari, M. (2018). The Concept of the Critical Information Infrastructure of the Russian Federation. In *ICCWS 2018: Proceedings of the 13th International Conference on Cyber Warfare and Security (Washington, DC, 2018),* pp. 543–551. Academic Conferences International.

III. Kari, M. (2018). The Protection of Russia's Critical Information Infrastructure. In *ECCWS 2018: Proceedings of the 17th European Conference on Cyber Warfare and Security (Oslo, 2018),* pp. 533–540. Academic Conferences International.

IV. Kari, M. (2019). Strategic Culture Theory as a Tool for Explaining Russian Cyber Threat Perception. In *ICCWS 2019: Proceedings of the 14th International Conference on Cyber Warfare and Security (Stellenbosch, 2019),* pp. 528–535. Academic Conferences International.

V. Kari, M. (2019). Protecting the Besieged Cyber Fortress: Russia's Response to Cyber Threats. In *Proceedings of the 18th European Conference on Cyber Warfare and Security – ECCWS 2019 (Coimbra, 2019),* pp. 685–691. Academic Conferences International.

VI. Kari, M. & Pynnöniemi, K. (2019). Theory of Strategic Culture: An Analytical Framework for Russian Cyber Threat Perception. Submitted to *Journal of Strategic Studies*.

The author of this thesis wrote Articles II–V. Article I was written with Adjunct Professor Rauno Kuusisto. Kari was the main contributor to Article I, and Kuusisto's role was to support and guide Kari in writing the first conference paper. Article VI was co-written with Assistant Professor of Russian Security Policy Katri Pynnöniemi at the National Defense University and Helsinki University.

The author of this thesis has presented the results of the articles at the following JuFo-1 level conferences:

Article I: 16th European Conference on Cyber Warfare and Security. Dublin, Ireland, 29–30 June 2017

Article II: 13th International Conference on Cyber Warfare and Security. Washington DC, USA. 8–9 March 2018

Article III: 17th European Conference on Cyber Warfare and Security. Oslo, Norway. 28–29 June 2018

Article IV:	14th International Conference on Cyber Warfare and Security. 28 February–1 March 2019, Stellenbosch, South Africa.
Article V:	18th European Conference on Cyber Warfare and Security. 4–5 July 2019, Coimbra, Portugal
Article VI:	Submitted to Journal of Strategic Studies without presentation at a conference.

1 INTRODUCTION

1.1 Russian Cyberspace and the Concept of Cyber Threat

Over the centuries, war has been, as Prussian military thinker Carl von Clausewitz (1832) defined it, “the continuation of politics by other means, with acts of violence to compel opponent to fulfill our will.” At the beginning of the 20th century wars were fought in a two-dimensional environment: the domains of warfare were land and sea. The operational use of airplanes in the First World War made air the third domain of warfare. After that, the role of air power has increased. Air force has a crucial role in warfare from tactical level to strategic level. Air power is a part of superpowers’ coercion and deterrence capabilities (Pape, 1996). Airplanes have been also used in terrorist attacks in an unpredictable way in the 9/11 attacks in 2001 in New York City. The launch of Sputnik in 1957, and the space flight of Major Yuri Gagarin from the Soviet Air Forces in 1961 were the beginning of converting space to yet another domain of warfare. At the start of this century, space has become the fourth domain and it is an integral part of military operations.

During 2000s, cyberspace matured to the fifth domain of warfare. (Drew, 2018). According to a Russian definition, cyberspace consists of the technological infrastructure, which enables the Internet and the functionality of other channels in telecommunication networks as well as of all the human activity that occurs on the Internet and via other communication channels (SBRF 2013). Today, cyberspace is not only a technical issue but it also has a strategic dimension. Conflicts have a cyber dimension and it is difficult to predict the size and impact of cyber components in the conflict (Geers, 2011). Cyberspace has expanded warfare to a global scale and beyond the traditional use of military force, and can be compared with the use of airplanes for terrorist attacks in the USA in 2001. The use of force in cyberspace to cause a strategic-level malicious impact does not demand state-level resources, as other domains of warfare do, with the exception of the 9/11 attacks.

Warfare in the cyber domain differs from warfare in other domains because actors in cyber conflicts are not always military. State actors, criminals and terrorists attack state authorities, media and critical infrastructure. State actors and private cybersecurity companies are fighting against these attackers. The attribution of attack to specific party is often difficult or impossible to do. In 2007, distributed denial of service (DDoS) attacks on Estonian government websites paralyzed public services for three weeks. In the Russian–Georgian war, in 2008, the website of the Georgian government and media were attacked. In 2010, Stuxnet malware damaged the centrifuges of Iranian uranium enrichment facilities in Natanz (CRC, 2016). The impact of the Stuxnet attack can be compared with the impact of attack by kinetic weapons because it destroyed a significant amount of centrifuges and delayed the uranium enrichment process. The NATO Warsaw summit in June 2016 declared cyberspace as a domain of warfare in which NATO must defend itself (NATO, 2016).

In June 2019, the USA administration admitted, that the USA has been conducted cyberspace exploitation operations in Russian power grid management systems at least since 2012 and prepared cyberspace attacks by installing “potentially paralyzing” malware in Russian information infrastructure. (Sanger & Perlroth, 2019) In response to this information, the Press Secretary for the President of Russia Dmitry Peskov stated, that hypothetically cyberwar between the US and Russia is possible. According to Peskov, Russia´s strategically vital areas of the economy were and are being subjected to cyber attacks from abroad and Russia is waging a constant struggle to prevent damage to the Russian economy and its sensitive areas. (Tass, 2019a) According to Russian officials, foreign intelligence agencies are attempting to infiltrate into Russia's information infrastructure systems, primarily in transport, banking and energy sectors. These actions were described as "elements of cyberwar." (Tass, 2019b)

The information security doctrine of the Russian Federation defines the threat to information security as a complex of actions and factors, creating a danger of damage to Russian interests in so-called information space (UP-646, 2016). Information space includes subjects creating, generating and processing information, subjects developing, using information technology, or managing information security. It also includes mechanisms regulating the information relations in society. Warfare in information space can be information-technical, when informational technical systems are objects of influence in cyberspace, or it can be information-psychological, when the adversary tries to influence a person’s mind, his or her moral and mental world, political opinions and ability to make decisions (Kamyshev 2009). The Russian definition of information-technical warfare is equivalent to the Western definition of cyber warfare. In both the objects of influence are technical systems in cyberspace.

This thesis examines Russian cyber threat perception and Russia’s response to that threat. In this thesis, cyber threat refers to those actions or factors which can cause serious harm in or through cyberspace. Cyber threats to the Russian Federation are a complex of actions and factors which either cause serious harm to interests of the Russian Federation or create the feeling of danger or real danger to serious harm to Russia's interests in or through cyberspace. Perception means a single unified awareness which is the basis for understanding and the motivation to act (Stein, 2013). Russia's cyber threat perception means Russian state-level unified awareness of the actions and factors which either cause serious harm to the interests of the Russian Federation or create the feeling of danger or real danger of serious harm to Russia's interests in or through cyberspace.

Russia's response to cyber threat means the implementation of mutually connected measures to predict, detect, suppress, prevent, and respond to cyber threats and mitigate their impact. These measures can be legal, organizational, investigative, intelligence, counter-intelligence, scientific and technological, information and analytical, personnel related, economic and others. The aim of these measures is to maintain and improve cyber security. Cyber security refers to the protection of cyberspace and the protection of those that function in cyberspace and of their assets that can be reached via cyberspace (Solms & Niekerk, 2012).

1.2 Previous Research

The Russian journalist Andrei Soldatov has published books on Russian security services and other security related topics. In 2015, he published The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries with Irina Borogan, where they describe the history of Russian Internet surveillance (Soldatov & Borogan, 2015). In 2017, Soldatov published an article in Russian Social Science "The Taming of the Internet," where he explains how the Kremlin has managed to place Internet companies operating in Russia under control and how Russian authorities have managed to build up systems for the mass surveillance of Russian internet users. According to Soldatov, however, state control remains incomplete. One reason is that, from its beginning, RuNet, the Russian portion of the Internet, developed as an open and free space and its infrastructure was built on Western technology, which had no built-in surveillance capabilities. In contrast to the Chinese Internet, RuNet was not originally developed inside something akin to China's "Great Firewall" (Soldatov, 2017).

Kenneth Geers has had an extensive professional and academic career related to cyber security, cyber warfare and cyber threats. He has published a book, Strategic Cyber Security (2011), and more than twenty articles and chapters on cyber security. He has also edited The Virtual Battlefield: Perspectives on Cyber Warfare (2009) and Cyber War in Perspective: Russian Aggression against Ukraine (2015).

Geers expands cyber threats and cyber security to the strategic level. In The Virtual Battlefield (2009), he states that traditional, strategic-level threats such as espionage, propaganda and attacks to critical infrastructure are today internet enabled. The use of cyberspace increases the speed, power and diffusion of these threats. He predicts that cyber warfare might have a lead role in conflicts of the future (Geers, 2009). In Strategic Cyber Security (2011), he argues that computer security has evolved from a technical discipline to a strategic concept and the dependence on Internet and cyberspace attacker´s disruptive capabilities threaten national and international security.

Keir Giles, from the Conflict Studies Research Centre, has published books and articles on military transformation in Russia, Russian foreign and domestic security policy and Russian information and cyber warfare. In the article he presented at the 4th International Conference on Cyber Conflict (CYCON 2012), "Russia's public stance on cyberspace issues," Giles (2012) examined the circulation of information, the perceived threat it poses to Russia, and Russia's digital sovereignty.

To describe and to explain the Russian public view on topics related to cyber security, Giles examines two documents, the Draft Convention on International Information Security (released in September 2011) and the Russian military cyber proto-doctrine Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space (released in December 2011). As a conclusion, he states that the Russian authorities considered protests in December 2011 as an information campaign against Russia.

In his 2013 study "Legality in Cyberspace: The Russian View," published by the Conflict Studies Research Centre, Giles explores the Russian approach to legal constraints of activities in cyberspace. According to Giles, Russian academic and military commentary sees the distinction between war and peace as now blurred and discusses at what point Russia should consider itself to be at war and subject to specific legal constraints on actions in cyberspace. In his article, "Legality in Cyberspace: An Adversary View," written with Andrew Monaghan and published by Strategic Studies Institute in 2014, Giles describes Russian views on the nature of conflict in cyberspace and explains how the USA needs to take into consideration Russian assumptions on the nature of cyber activity when engaging with Russian cyber initiatives. In his articles, Giles discuss the Russian view on the nature of conflict in cyberspace, but he does not using the theory of strategic culture to explain the factors influencing elements of Russian state behavior in cyberspace.

Carolina Vendil Pallin from the Swedish Defence Research Agency (FOI) has published four books and multiple articles on military thinking and Russian military reform as well as on Russian information security and warfare. With Ulrik Franke, she has published the report Russian Politics and the Internet in 2012. The authors discuss how the wave of protests in Russia after the 2011 parliamentary elections and the 2012 presidential election demonstrated to Russian leadership the political role of the Internet for distributing information and calling people to participate in demonstrations. After these events, a number of laws have come into force to block and censor websites including harmful content and to increase Internet surveillance (Vendil Pallin & Franke, 2012).

In 2016, Vendil Pallin (2016) published an online article in Post-Soviet Affairs, "Internet Control Through Ownership: The Case of Russia." This article is a continuation and update of a study published in 2012 (Vendil Pallin & Franke, 2012). It describes how the Russian Internet remained relatively unregulated until about 2012 and how the Russian government started to control the Internet through ownership over the Russian Internet companies (Vendil Pallin, 2016).

In her article "Russian Information Security and Warfare," published in the Handbook of Russian Security (2019) Vendil Pallin provides a good insight to Russian cyber security strategies, doctrines and legislation, organizations and the implementation of cyber security. Vendil Pallin also describes Russian leadership's pivot to balance between the need to control RuNet and to protect users' privacy and freedom.

Lincoln Pigman at the University of Oxford has published articles on the control of Russian cyberspace. In 2018, Pigman (2018) published the study "Reining In the Runet: The Kremlin's Struggle to Control Cyberspace," in which he has collected Russian legislation controlling RuNet. According to Pigman, Russian leadership decided to take RuNet under state control in 2011–2012, because they were afraid that an Arab Spring-type of revolt could happen in Russia as well. Pigman describes how new laws increased control of RuNet by, for example, restricting Internet users' access to problematic information and limiting Internet users' anonymity. Pigman does not apply the theory of strategic culture in his study.

The Finnish Defence Research Agency has published collections of articles edited by three researchers, Juha Kukkola, Mari Ristolainen, Juha-Pekka Nikkarila, who are representatives of the Finnish Defence Research Agency and the National Defence University. Russia's cyber threat perception and Russia's response to that threat are both addressed in Game Changer: Structural Transformation of Cyberspace (2017) and Game Player: Facing the Structural Transformation of Cyberspace (2019). Game Changer contains six peer-reviewed articles and Game Player eight articles. The articles were first published by cyber security conferences such as the International Conference of Cyber Warfare and Security (ICCWS), the European Conference of Cyber Warfare and Security (ECCWS), the International Conference on Military Communications and Information Systems (ICMCIS 2017), and Military Communications (MILCOM 2017), and the International Command and Control Research and Technology Symposium (ICCRTS 2017).

In Game Changer, the authors discuss topics such as RuNet 2020 and the asymmetric frontlines caused by a closed Russian network. The authors argue that the development of RuNet 2020 can be analyzed with conventional military tactics and means in deploying traditional elements of warfare in cyberspace, to improve maneuverability and firepower. One of the authors is also modelling the imbalance of cyber operations between closed and open national networks. Game Changer comes to the conclusion that the goal of a closed network is related to enhancing military capabilities by achieving a higher operational capability than an open network. The authors also discuss digital sovereignty, which refers to Russia's rights to independently determine internal and geopolitical interests in the digital space (Yarovaya, 2013).

In Game Player, the authors have divided the articles into four sections. The first chapter, "State of the Game," contains the article "Russian Cyber Power and Structural Asymmetry", where Juha Kukkola presents the concept of structural cyber asymmetry and explains how Russians perceive cyber power, including the shaping of strategic cyberspace. In the first article of the second chapter called Understanding the Game Board, Kukkola discusses how Russia is preparing to protect Russian national segment of the Internet, and how this may change the military balance in cyberspace. This article includes an interesting table on actors, elements and responsibilities of actors of RuNet.

In the second article of this section, "Projected Territoriality: A Case Study of the Infrastructure of Russian Digital Borders," Kukkola discusses with Mari Ristolainen about delineation and the protection of digital borders and how territoriality can be projected into cyberspace. In the next article, "New guidance for preparing Russian 'digital sovereignty'" Kukkola analyses the Program of the Digital Economy of the Russian Federation and its action plans approved at the beginning of 2018 and demonstrates that Russian 'digital' socio-economic plans also include a military strategic character. The article "Modelling closed national networks – Effects in cyber operation capabilities," written by Juha-Pekka Nikkarila, Bernt Åkesson, Vesa Kuikka and Juhani Hämäläinen, introduces a mathematical model of how operational capabilities can be estimated when a national network is closed.

Kukkola's article "The Russian Segment of the Internet as a Resilient Battlefield concludes the second section. In this article, Kukkola claims that Russia is building a system-of-systems of cyber security to withstand cyber-attacks against its critical national assets. The article also analyses the resilience of the national segment of the Internet and argues that Russia is aiming for a flexible cyber defense system providing advantage in a cyber conflict.

The third section is called "Playing the Game," and it includes two articles, "Wargaming a Closed National Network: What are You Willing to Sacrifice?" and "Wargaming the Cyber Resilience of Structurally and Technologically Different Networks." Both of these two articles discuss wargaming in cyberspace. In the epilogue Margarita Jaitner and Teodor Sommestad, researchers from the Swedish Defence Research Agency (FOI), highlight that the authors of Game Player "have conducted an extensive, invaluable investigation into Russian efforts and provided actionable alternatives for handling the resulting challenges."

Both Game Changer and Game Player provide extensive information, and they give the reader a broad and deep understanding on Russia's plan to improve the country's digital sovereignty by preparing to isolate RuNet from the global Internet. The books also present a mathematical model for estimating the consequences of closed networks in wartime. The authors have been concentrated on cyberspace and there has not been any discussion on the general and strategic factors influencing Russian policy to improve digital sovereignty except the strategic level military factors. The authors of Game Changer and Game Player have not applied the theory of strategic culture and Russian strategic culture as an interpretative tool. Russian strategic culture is mentioned in these two books once as a term, when the Finnish synopsis of Game Player states the following:

> The main statements and research results presented in this article collection are as follows. Russia's ambition to remove its national segment from the global Internet leads to structural asymmetry and it is a reflection of Russian strategic culture.[1]

Even though both books contain excellent studies, there remains a need to study Russian strategic culture generally and Russian strategic culture in cyberspace to explain and to assess the Russian state's behavior in cyberspace.

1.3 Cyber Security Research

Information Systems (IS) science consists of several different fields of research and is by nature both social and technical. The research area of information systems includes a number of different topics concerning the technology, development and management of information systems or their organizational or social impact. IS science is interested in the utility of information technology in the daily activities of individuals and organizations. The aim of IS science is to understand information systems from the perspective of technology, users and information systems (JYU, 2019).

Information system security (ISS) means protecting information and information systems from unauthorized use, access, modification or removal. ISS research started in the 1970s and the first studies were practical problem-solving descriptions and guidelines for practice. The first generation of ISS researchers in the 1970s provided limited solutions to information problems with security checklists and risk analysis. In the 1980s, the second generation's mechanistic engineering methods replaced these first generation checklists and risk analysis. At the end of the 1980s, the third generation developed ISS through logical controls design and data flow diagrams as well as ISS maturity and management standards including best solutions and practices for ISS management problems. (Baskerville, 1993)

Cyber security is a part of IS science and a subset of information security. It focuses on protecting computer systems and digital infrastructure from digital attacks. Cyber security consists of technologies, processes and controls designed to protect systems, networks, programs, devices, and data from cyber-attacks. Effective cyber security reduces the risk of cyber-attacks and protects information systems against the unauthorized exploitation of systems, networks and technologies. (IT-Gov, 2018)

[1] Kukkola, Ristolainen & Nikkarila, 2019

According to the Russian cyber security company Kaspersky (2019), cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Cyber security can be called also as information technology security or electronic information security. Cyber security can be divided into five categories. Network security means securing a computer network from intruders; operational security means the processes and decisions for handling and protecting data assets. Disaster recovery and business continuity define means and methods to respond to a cyber-security incident and to return to the same operating capacity as before the event.

Cyber security is the practice of protecting information and data and the protecting of networks, servers, intranets and computer systems. The purpose of cyber security research is to understand the cyberspace, cyber threats, countermeasures against cyber threats, and the preparation of society for cyber crises. In some cases, cyber security researchers do not have expertise in tools and methods of social science. Human behavior affects all stages of the cyber security system from design to operation and maintenance. Effective cyber security means understanding and addressing the human dimensions of systems. Integrating this understanding about human nature with more traditional cyber security research related sciences such as computer and engineering sciences and mathematics creates a more solid cyber security science. (Millett et al., 2017)

This thesis on Russian cyber threat perception is ISS research. It combines technical and social aspects as well as discusses the relationship between information technology and the organization that utilizes it. The purpose of this thesis is to understand information systems—in this case, the Russian information systems, and especially the country's cyber threat perception and protection of information and information systems against cyber threats. This thesis is a combination of information system science, international law, history, international politics, Russian studies and military sciences. It requires that a researcher has good knowledge of Russian, because the primary data are in Russian.

Siponen and Baskerville (2018) presents a division of ISS research into four levels: the metalevel, basic, applied and post-intervention research. The key issues of metalevel research are definitions that guide research on ISS phenomena. Basic level ISS research provides fundamental explanations for ISS phenomena and detailed understanding of the meaning of these explanations in different contexts. The goal of applied research is to direct basic research to practical, applicable results. Post-intervention research explains the results of interventions implemented in applied research to test the effect rate (Siponen & Baskerville, 2018). This thesis is basic level research exploring how the theory of strategic culture can be used to explain the phenomenon of Russian cyber threat perception. This thesis provides a fundamental explanation based on the theory of strategic culture for Russian cyber threat perception and understanding the meaning of this theory in cyberspace.

The articles of this thesis have been published in the proceedings of the European Conference on Cyber Warfare and Security (ECCWS) and the International Conference on Cyber Warfare and Security (CCWS) as well as in Journal of Strategic Studies. The European Conference on Cyber Warfare and Security (ECCWS) and International Conference on Cyber Warfare and Security (CCWS) are the two main conferences for academics and practitioners to present their empirical studies, case histories and other theoretical and practical contributions on cyber warfare and cyber security. In addition, doctoral degree candidates have an opportunity to present their papers and posters. The first ECCWS was organized in 2001 and the first ICCWS was organized in 2005. The conferences are generally attended by participants from more than 30 countries. The Journal of Information Warfare regularly publishes a number of the papers presented at these conferences (ECCWS, 2019; ICCWS, 2019). Journal of Strategic Studies, first published in 1978, is a multi-disciplinary review of forward-looking articles on military and diplomatic strategy, that is, on strategic studies. It is published six times per year.

1.4 Research Questions, Objectives and Approach

The increased interest in cyberspace as an arena of international politics has also heightened the need for theoretical tools and methods to estimate cyber threat perceptions of different states and responses to cyber threats. This thesis suggests that Russian cyber threat perception and Russia's response to the cyber threat can be constructed and explained by correctly selecting and using documents, tools and methods, even if the state's real threat perception is not public. Finding answers to strategic-level questions on the cyber threat demands a multidisciplinary approach.

Grounded theory was used to collect and to code the data. Grounded theory is a systematic methodology in the social sciences involving methodical gathering and analysis of data. Grounded theory was also used to construct a model of Russian cyber threat perception and Russia's response to the cyber threat. The theory of strategic culture, a theory used in studies of international relations and politics, was used to explain the constructed model of Russian cyber threat perception. The version of the theory of strategic culture used in this thesis is that developed by Alastair Iain Johnston in the 1990s. Even though Johnston's analytical framework is almost 25 years old, it was selected as the theory for this thesis because Johnston's approach is still valid. The division of strategic culture into a central paradigm and strategic preferences provides a sufficient framework to explain the Russian cyber threat perception and the country's response to cyber threats. The central paradigm of Russian strategic culture corresponds to the Russian threat perception and strategic preferences correspond to Russia's response to such threats. This applies in cyberspace as well.

Only a limited amount of information has been published about the Russian defensive cyber capabilities and Russian cyber threat scenarios. However, there is information enough in official Russian documents to build up a description of the Russian perception of cyber threats and Russia's response to that threat. The Russian cyber threat perception and planned measures to fight this threat can be found in the official Russian documentation such as drafts of laws, laws, presidential and governmental decrees, doctrines, strategies and other documents related to Russia's information security management.

These Russian official documents related to cyber security can be considered reliable valid primary sources, because they are used by Russian authorities to describe the cyber threat environment as well as to give guidance to Russian society and people to counter these threats. Even though the detailed cyber threat picture is classified, official documents had to include information close enough to the real, classified picture to give realistic enough information to counter the cyber threat. Grounded theory has been a suitable tool to review and collect scattered information in official documents and to build up a description of the country's perception of cyber threats.

Furthermore, this thesis argues that strategic culture theory is suitable for explaining Russian cyber threat perception and the response to those threats. The aim of this thesis is to develop, through the use of the theory of strategic culture, context-based, process-oriented description and explanation of the Russian perception about the cyber threats and Russia's counter-measures against these cyber threats. The research questions are

- What is Russia's cyber threat perception?
- What are the most important objects to protect in Russia's cyber threat perception?
- How is Russia responding to cyber threats?
- How does Russian strategic culture explain Russia's cyber threat perception and response to cyber threat?

1.5 The Research Process

1.5.1 A Model of Russian Cyber Threat and Response

The research process of this thesis consists of three main phases. The first phase was carried out by using grounded theory as a method to construct a model of Russia's perception of cyber threats and the country's response to cyber threats. This model includes the following elements: object and subject of cyber threats; the tactics, techniques and procedures (TTP) of cyber threats; and the possible consequences caused by a cyber threat if realized. The model also includes the object, subject and aim of cyber defense; the TTP of cyber defense; and limitations of Russia's cyber defense. The model of Russia's perception of cyber threats and response is presented in Figure 1. The process of establishing the model by using grounded theory is discussed in more detail in Chapter 2.

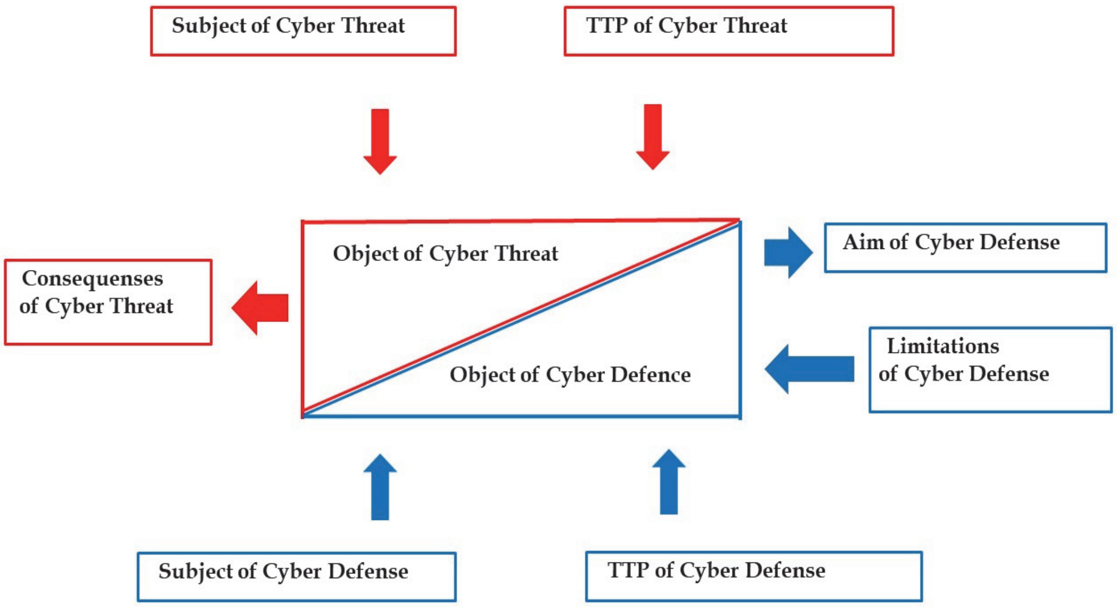


FIGURE 1 A model of Russian cyber threat perception and response to that threat

The first phase of the study has been implemented in Articles I and V, while the definition and protection of the critical information infrastructure of the Russian Federation is addressed in Articles II and III. The result of the first phase is a pattern, a model of cyber threats to Russia and Russia's response to cyber threats, including description of the most important objects to protect. The research questions of the first phase are the following:

- What is Russia's cyber threat perception?
- What are the most important objects to protect in Russia's cyber threat perception?
- How is Russia responding to cyber threats?

These research questions are answered in Chapter 4 and as well as in Articles I, II, III and V.

1.5.2 Factors and Elements of Russian Strategic Culture

The second phase of the study examines Russian general threat perception. The aim of the second phase is to identify and describe the factors influencing elements of Russian strategic culture. The elements of strategic culture are the central paradigm and a set of strategic preferences. The central paradigm includes assumptions about the nature and role of the conflict and the enemy, and about the threat posed by the enemy. Strategic preferences mean the assumptions how to deal with these threats. The theory of strategic culture is discussed in Articles IV and VI, and in Chapter 5. The interconnection of factors and elements of Russian strategic culture is described in Figure 2.

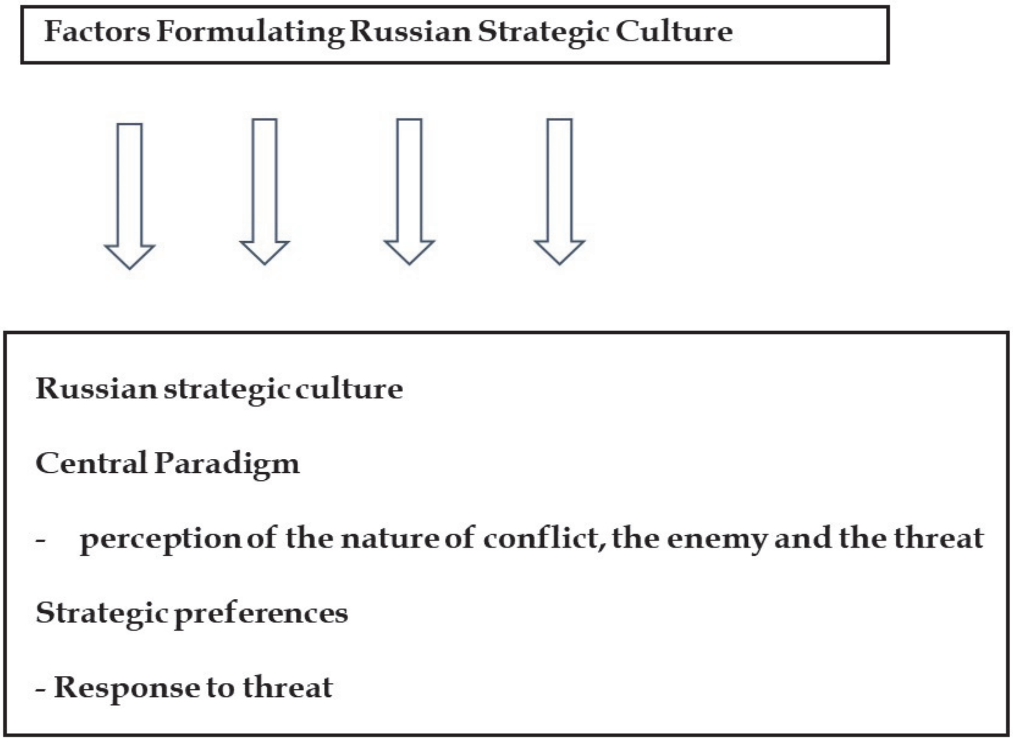

Factors Formulating Russian Strategic Culture
Russian strategic culture
Central Paradigm
- perception of the nature of conflict, the enemy and the threat
Strategic preferences
- Response to threat

FIGURE 2 Interconnection of factors and elements Russian strategic culture

Johnston (1995b) sees that one productive way to identify a central paradigm and strategic preferences is to analyze the content of recent texts related to the subject in question. The central paradigm of Russian strategic culture can be observed in subject-related high-level documents, such as strategies and doctrines. Because the researcher does not have insight into how strategic preferences are implemented in practice, their implementation had to be exposed and explained by describing the content of doctrines and more practical-level documents such as laws and guidance documents of different security-related state organizations.

1.5.3 Elements of Russian Strategic Culture in Cyberspace

The third phase of the study argues that the theory of strategic culture is a suitable theory for exploring and explaining the Russian vision of cyber conflicts, its enemies, cyber threats and preferences for responding to cyber threats. Russian cyber threat perception is not a separate aspect of Russia's general threat picture. Factors of Russia's strategic culture also influence the country's strategic culture in cyberspace. Figure 3 presents the relationship between factors and elements of Russian strategic culture and the factors and elements of Russian strategic culture in cyberspace.

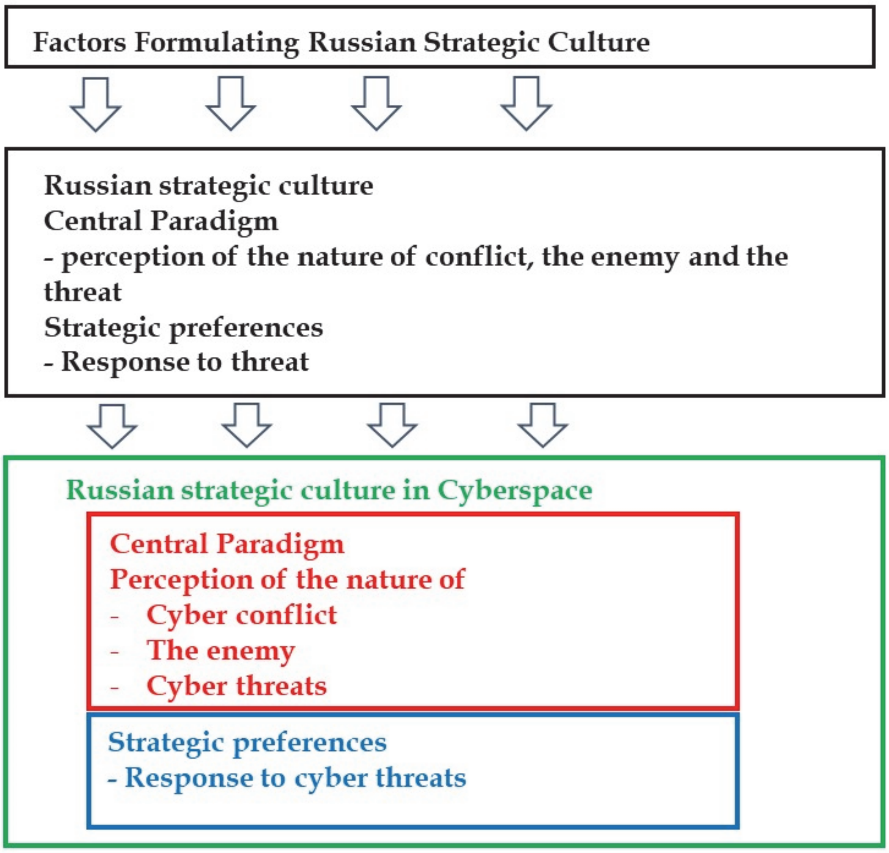

Factors Formulating Russian Strategic Culture
Russian strategic culture
Central Paradigm
- perception of the nature of conflict, the enemy and the threat
Strategic preferences
- Response to threat
Russian strategic culture in Cyberspace
Central Paradigm
Perception of the nature of
- Cyber conflict
- The enemy
- Cyber threats
Strategic preferences
- Response to cyber threats

FIGURE 3 Factors and elements of Russian strategic culture and factors and elements of Russian strategic culture in cyberspace

The central paradigm of Russian strategic culture in cyberspace includes assumptions about the nature and role of cyber conflict and the enemy, and about the cyber threat posed by the enemy. Russian strategic preferences in cyberspace mean assumptions about how to deal with cyber threats.

In the third phase, after discussion on Russian strategic culture in cyberspace, the factors and elements of Russian strategic culture in cyberspace are used to explain the model of Russian cyber threat and response. The central paradigm of Russian strategic culture explains the country's cyber threat perception and its strategic preferences explain its response to those threats. Russian cyber threat perception and response through the lens of Russian strategic culture is described in Figure 4.

Interpretation of the model of Russian cyber threat and response is described in Figure 4, and discussed in Articles IV and VI, and in Chapter 5. This phase of study answers the research question

- How does Russian strategic culture explain Russia's cyber threat perception and response to cyber threats?

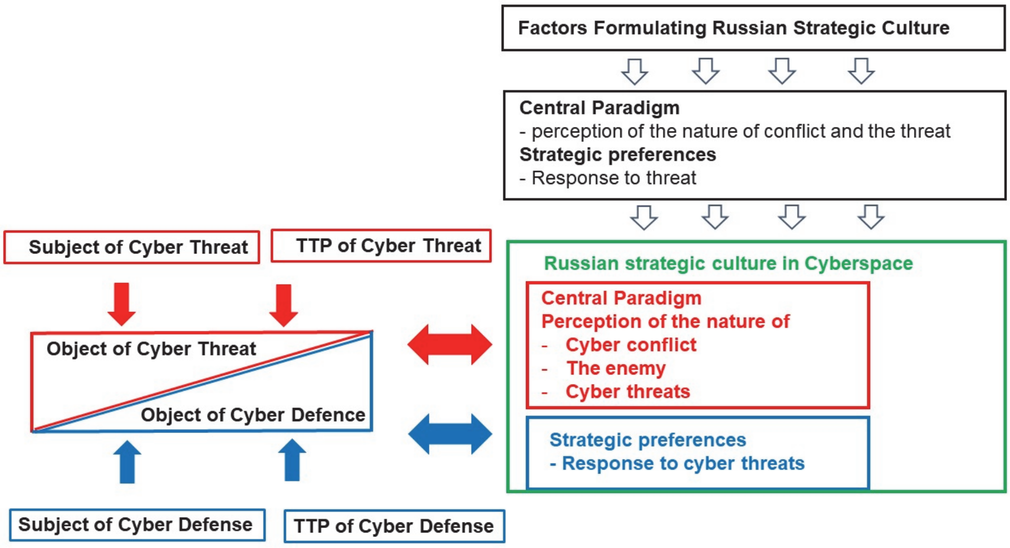


FIGURE 4 Interpretation of the model of Russian cyber threat

1.5.4 Relationship of the Included Articles

This thesis contains six articles discussing the research objectives from different viewpoints. The interconnection of the articles is presented in Figure 5. The articles are numbered in chronological order based on time of publication. Article I is oldest, and Article VI is the newest.

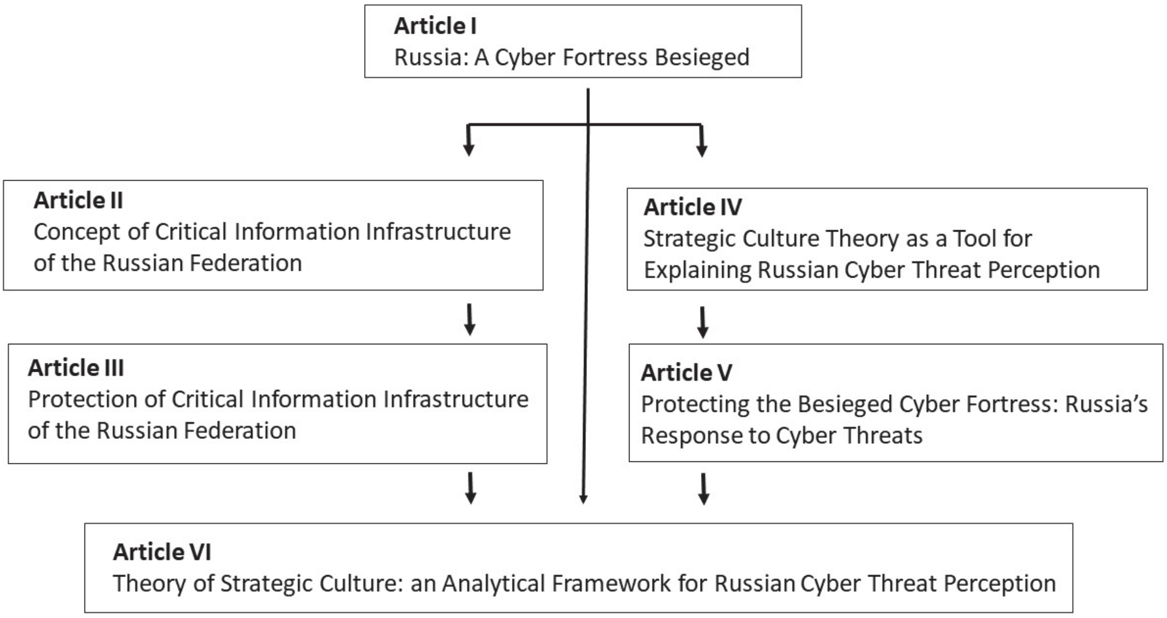
Article I, “Russia: A Cyber Fortress Besieged,” is a general introduction to Russian cyber threat perception. The information in Article I on critical information infrastructure is updated in articles II and III and that on Russian cyber threat perception and Russia’s response to that threat in articles IV and V. Article I answers research question “What is Russia’s cyber threat perception?”.

Article II, “The Concept of the Critical Information Infrastructure of the Russian Federation,” examines the evaluation of the concept of Critical Information Infrastructure of the Russian Federation. The aim of Article II is to describe the process of evaluation of the concept of Russian critical information infrastructure. Article III, “The Protection of the Critical Information Infrastructure of the Russian Federation,” is a continuation of Article II. Together with Article II, Article III constitutes one of the main topics related to the question of what, according to Russia’s cyber threat perception, are the most important objects to protect. Articles II and III answer research questions

- What are the most important objects to protect in Russia’s cyber threat perception?
- How is Russia responding to cyber threats?

Article IV, “Strategic Culture Theory as a Tool for Explaining Russian Cyber Threat Perception,” argues that strategic culture theory is a suitable tool for exploring and explaining the Russian idea of cyber conflicts, the country’s cyber threat perception and its strategic preferences, that is, its options to respond to cyber threats. Article IV is complemented and focused by Article VI. Article IV answers research question “How does Russian strategic culture explain Russia’s cyber threat perception and response to cyber threat?”. Article V, “Protecting the Besieged Cyber Fortress: Russia’s Response to Cyber Threats,” discusses Russia’s defense against cyber threats and answer research question “How is Russia responding to cyber threats?”.

Article VI, “Theory of strategic culture: An Analytical Framework for Russian Cyber Threat Perception”, comprises the theoretical background of this thesis. Article VI argues that the theory of strategic culture is suitable to explore and to explain the formation of Russian cyber threat perceptions and the country’s subsequent cyber strategy. Article VI formulates an analytical framework to study the formation of Russian thinking on cyber threats as a part of Russian strategic culture. Article VI discusses all the four research questions.



Article I
Russia: A Cyber Fortress Besieged

Article II
Concept of Critical Information Infrastructure of the Russian Federation

Article III
Protection of Critical Information Infrastructure of the Russian Federation

Article IV
Strategic Culture Theory as a Tool for Explaining Russian Cyber Threat Perception

Article V
Protecting the Besieged Cyber Fortress: Russia’s Response to Cyber Threats

Article VI
Theory of Strategic Culture: an Analytical Framework for Russian Cyber Threat Perception

FIGURE 5 Interconnection of the articles and the structure of the study

2 METHODOLOGY

2.1 Selection of Grounded Theory as a Method

The method used in this thesis to coordinate and guide the data collection, and then to parse and structure the data themselves, is grounded theory. Grounded theory was selected because it is well suited for studying phenomena about which theoretical and structured information is lacking but which is needed, for example, to support professional decision-making or basic research (Koskennurmi-Sivonen, 2007). A limited amount of theoretical and structured information has been published about the defensive cyber capabilities of Russia and Russian cyber threat scenarios. Such information is needed for both basic research and professional decision-making in the areas interested in Russian cyber defense.

Grounded theory is well suited for research that aims to create new knowledge with qualitative material (Strauss & Corbin, 1998). It also provides perspective on the behaviour of the object and helps construct a pattern or system, consisting of groups of logically interrelated concepts (Birks & Mills, 2015). The aim of this thesis is to create new knowledge on the Russian cyber threat perception using grounded theory as a tool to construct a perspective on this perception and as well as on Russia's behaviour and pattern in responding to this threat.

This thesis adopts the version of grounded theory developed by Anselm Strauss and Juliet Corbin (1990). Compared with the original version of the theory, the Corbin-Strauss version is more structured. It assumes that the researcher is already familiar with the theoretical literature related to the studied subject. In contrast to Glaser's improvisation- and intuition-orientated version, where the researcher should avoid the theoretical subject-related literature at the beginning of his study to prevent the formation of unconscious bias about the research subject, in the Corbin-Strauss version the research problem is defined deductively in advance. Corbin and Strauss were also in favour of predetermined coding parameters, a systematic approach and the structural analysis of information.

I have reviewed the theoretical literature related to the studied area in my professional career and during the process of completing my master's thesis. The Corbin-Strauss version of grounded theory was selected as a method even though it has developed since 1990s, when Corbin and Strauss created their interpretation of it. In 2000, Kathy Charmaz developed constructivist grounded theory. The main way of collecting the data in constructivist grounded theory is intensive interviews, which was not an appropriate approach to data collection in this thesis. To avoid philosophical debates on the superiority of different versions of the theory, the Corbin-Strauss version has been selected because it is suitable for constructing a pattern, in this case, a description of Russian cyber threat perception and Russia's response to that threat.

Grounded theory is a method of systematically examining qualitative data such as interview records, protocols, or documents with the aim of forming a model. The primary data used in this thesis consists of different Russian official documents as the Russian Federation's laws and presidential decrees. Secondary data and supporting material include commentary by Russian and Western specialists on the topic. The data is discussed in more detail in Chapter 3.

2.2 The Evolution of Grounded Theory

The evolution and development of grounded theory should be understood as an evolution process, which began from original text of Glaser and Strauss and continues today. Grounded theory was developed in the 1960s in the United States, where social theory was dominated by a traditional theory-based research method. In this approach, the theory was chosen first, and then the collected material was placed in this model. This requires the existence and use of accurate and clear theory before data collection. As a result, the study did not produce new theories or new concepts (Kelle, 2005).

Sociologists Barney Glaser and Anselm Strauss considered the tasks related to the development of theories neglected. In response to the traditional theory-based research method, they developed a material-based analysis to form and develop new social theories. Glaser brought the quantitative research methods of Columbia University's sociological research to the theory. Strauss introduced the "symbolic interactionalists" tradition of qualitative research from the University of Chicago (Dey, 1999). Glaser and Strauss first used a new continuous comparison method in 1965 in their study Awareness of Dying (Kenny & Fourie, 2014).

The basic idea of the continuous comparison of Glaser and Strauss was to discover the theory from data (Glaser & Strauss, 1967). Glaser and Strauss introduced their theory, which they named grounded theory, in 1967 in their book The Discovery of Grounded Theory: Strategies for Qualitative Research. Subsequently, they published two studies based on grounded theory: Time for Dying in 1968 and Status Passage in 1971 (Kenny & Fourie, 2014).

In the early 1980s, differences of opinion about how to apply grounded theory began to emerge between Glaser and Strauss. Each began to develop the theory in different directions, for example, regarding coding techniques and interpretation models. Strauss tied his own model to the interactive theory of action and developed a coding paradigm model based on this theory (Birks & Mills, 2015).

Strauss and his pupil and co-worker Juliet Corbin considered that the original grounded theory approach overly emphasized an inductive approach. In addition, the use of Strauss's paradigm as an analysis tool seemed a good solution. (Strauss & Corbin, 1990; Strauss & Corbin, 1994). The organized form and phases of the paradigm support and guide the work of the novice researcher.

Glaser emphasized material orientation and developed a more formal conceptual model than the Strauss model contained. The model was intended to be theoretically more open and aimed at ensuring the nature of analysis, evolving from the data (Silvonen & Keso, 1999). The differences in opinions increased when Strauss published Qualitative Analysis for Social Scientists (1987) and, together with Corbin, Basics of Qualitative Research: Grounded Theory Procedures and Techniques (1990).

In response to Strauss and Corbin's work, Glaser published Basics of Grounded Theory Analysis: Emergence vs. Forcing (1992). In the book, Glaser explains why the theory developed by Corbin and Strauss is not grounded theory in its original and intended form but a form of qualitative data analysis (Cooney, 2010; Dey, 1999).

Glaser criticized Strauss's methodology because its predetermined way of working distorts too many interpretations. In addition, according to Strauss's view, a predetermined research problem is a kind of identifier of the phenomenon being researched. According to Glaser, the research problem should in no way be too pre-defined in advance, but should give rise and define itself as a kind of by-product as the research progresses (Babchuk, 1996). Glaser supported the openness, improvisation, intuition, reasoning, creativity, openness, and creativity of the researcher within the process steps of the method and the working methods. Glaser's idea was to avoid any predetermination in the early stages of the research and let the material and the research modify the way in which the research proceeds. According to Glaser, the researcher should not be bound to and confine himself to the research material, but the data is everything that comes to the researcher's mind. In Glaser's view, predetermined data analysis methods lead to theories based on preconceptions (Dey, 2001).

Glaser recommends avoiding theoretical literature in the early stages of the research, so that the researcher does not acquire unconscious assumptions about the research topic. The material and researcher's interaction with material must be adapted to the way in which the research progresses (Cooney, 2010).

Straussian grounded theory consists of three coding phases: open coding, axial coding, and selective coding. Coding means that the researcher conceptualizes the issues, he has discovered in the material, constantly collects material related questions and constantly compares his findings with the material already analyzed (Corbin & Strauss, 2008).

The phases of coding are not consecutive but partially overlapping. Open coding and axial coding may overlap in the same encoding event. For example, if a concept emerges in the final phase of selective coding which is poorly described or integrated, the researcher may have to return to open or axial coding (Corbin & Strauss, 2008).

The collection of data, data analysis and the formation of concepts, categories and interconnecting relationships between them are not separate events, but partly overlapping. Data analysis can be started as soon as the data collection begins. The researcher can return to collecting data until saturation, meaning until new categories affecting the data are no longer found (Birks & Mills, 2015). Saturation indicates that new material that could further develop a category's attributes can no longer be found (Glaser & Strauss, 1967).

The analysis steers and directs the data collection. When gaps are detected during the data analysis, the collection can be directed to fill these gaps. The researcher constantly compares new material with the material already analysed and seeks similarities and differences between concepts and categories (Strauss & Corbin, 1998). The researcher can also compare his own material and the results of the study already reported in the technical literature. If conflicts are detected in the comparison, it is relevant to find the cause of this deviation (Corbin, 2008).

Constructivist grounded theory is based on the assumption that neither data nor theory are discovered, but are constructed by researchers in their interactions with the field of study and research participants. Charmaz's (2014) idea is to keep the researcher close to the participants and the participants present in the coding phase by keeping their words intact in the process of analysis. In constructivist grounded theory, the main method of data collection is intensive interviews. The evolution of grounded theory is presented in Figure 6.

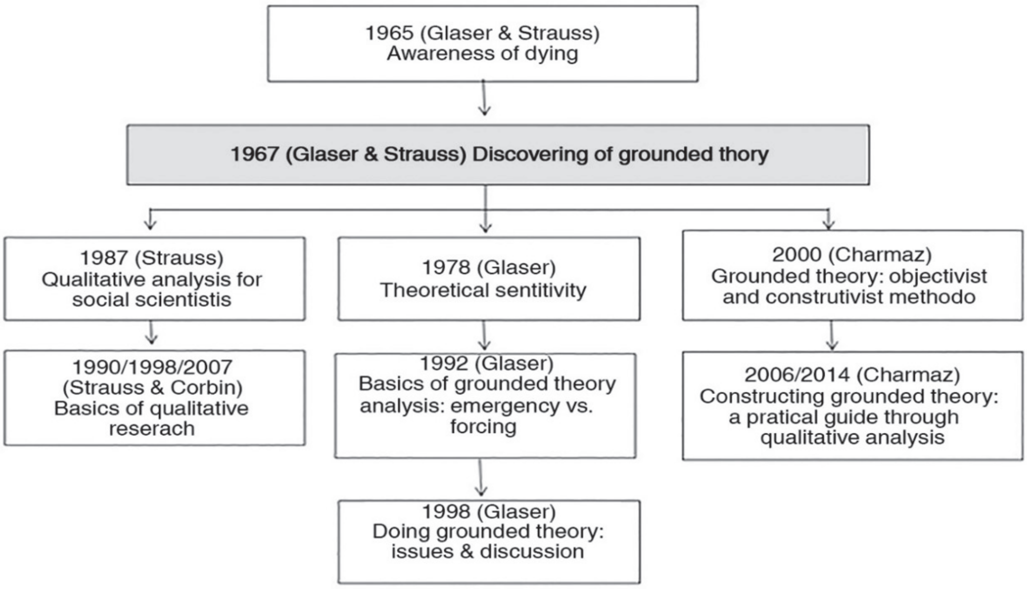


FIGURE 6 The Evolution of Grounded Theory (Glaser, 2011)

2.3 The Process of Grounded Theory

2.3.1 Open Coding

According to Corbin and Strauss (1990), the first phase of the coding in grounded theory is open coding. In open coding, the researcher collects and analyses data. The analysis directs the data collection and if gaps are detected in the data, the collection can be directed to fill these gaps. The researcher starts to make content codes, that is, concepts. The concept is an idea or an image that includes an explanation of the phenomenon or its characteristics. Conceptualization means giving the subject a descriptive name (Corbin, 2008). The concept then refers to a phenomenon that represents a particular event, activity, actor or matter (Strauss & Corbin, 1998). Open coding means conceptualization, fragmentation and reformatting or structuring of the data (Saaranen-Kauppinen & Puusniekka, 2009). In open coding, the source material is carefully read. The aim is to find basic concepts related to the subject being studied and define their features and dimensions.

The conceptual name is an expression that describes the subject that has emerged on a more general level. If a similar subject appears in the data, called in a different way, it is coded under the same concept. A conceptual name may come from research literature, professional experience or it may be material-based (Koskennurmi-Sivonen, 2007).The concept is an idea or an image that includes an explanation of the phenomenon or its characteristics. The use of concepts allows grouping the material into categories. The lower-level concepts form the basis for the grouping of the higher-level concepts (Birks & Mills, 2015). As examples of lower-level concepts, Corbin includes bird, airplane and kite.

Higher-level concepts include, for example, flying. Initial analysis consists of an open and free approach similar to "brainstorming" (Strauss & Corbin, 2008).

The researcher starts to form categories of information about the studied phenomenon from the concepts by grouping the information into dimensionalized categories. The first phase of the coding in grounded theory is described in Figure 7. Open coding is a compilation of hypotheses about the categories that the material produces. A rough first definition of the phenomenon is created to be investigated. In open coding, the aims of data collection (i.e. theoretical sampling) are to identify concepts and categories. The collection is called open because the value of each piece of material is not necessarily known in the beginning. For this thesis the collection started in 2015 and the value of each collected piece of material was clarified during the sampling process. In open coding, documents are not structured or categorized too strictly. It is important to maintain a balance between already collected material and new discoveries (Corbin & Strauss, 1990).

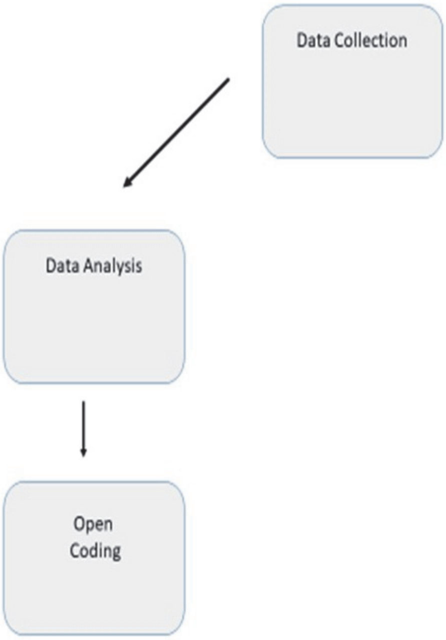


FIGURE 7 The first phase of the coding in grounded theory

In open coding the concepts are used to group and categorize the collected data into categories. In categorization, the concepts are grouped into categories, which are groups around the corresponding phenomenon (Corbin, 2008). Dey (1999) gives two examples of the categorization of concepts cat, dog and bone. According to the similarity categorization, cat and dog belong to the same animal category. According to the categorization based on connection, the dog and the bone, representing a dog's food, belong to the same category. Interdependencies between concepts do not always have to be logical, but they must be clear (Dey, 1999). Open coding continues until the categories begin to form. The source text is carefully studied in order to find and take into account all possible categories and sub-categories (Birks & Mills 2015).

The category is individualized by giving the category a more abstract name than the name of concept, which represents the phenomenon. The name may be taken from literature or from data. The problem is that, for example, the name of a concept or a category taken from technical literature already includes meanings and associations that can mislead the researcher because of the prediction assumptions (Corbin, 2008). The category is multidimensional and may include several subcategories (Birks & Mills, 2015, 15). The category is the element of theoretical reading (Glaser & Strauss, 1967). This means that the categories in grounded theory are more than just names or affixes attached to their identifiers (Dey, 1999). The name of the category may come from research literature or professional expertise.

2.3.2 Axial Coding

In open coding, the researcher breaks the data into pieces, and identifies and names the concepts from which the categories are constructed. In axial coding, categories are assembled into a visual model. The aim of axial coding is to search for one or more core categories that may be present in the data, to define relationships between categories and sub-categories, and thus to create clarity for the conceptual system being developed. Axial coding combines sub-categories into categories and combines categories with each other. In addition, in axial coding, the phenomenon is studied in a wider context including activity, interaction and causation (Strauss & Corbin, 1998)

Axial coding creates connections and links between the concepts and categories created in open coding. The researcher identifies a core category. Core categories represent the main theme of the research and has the greatest explanatory relevance and highest potential for linking other categories together (Strauss & Corbin, 1998). The core category is a category, which frequently occurs in the data and is logical, coherent and consistent with the rest of the data (Strauss & Corbin, 1994). The core category describes the core idea of the research. The criteria for choosing a core category are as follows (Strauss & Corbin, 2008):

- should be abstract
- other main categories can be attached to the core category, and other categories placed under the core category
- must occur regularly in the data being investigated
- must be logical, and compliant and consistent with the data
- must be abstract enough that it can be used in another study
- must be consistent with the research question
- must adapt to the theoretical framework of the study

The researcher constantly compares new material with the material already collected and analysed and seeks similarities and differences between concepts and categories. In this second phase of the coding, categories are assembled into a visual model. The aim is to deepen each category. Encoding takes place centrally around the selected elements, the so-called axes. The researcher then identifies a core category. The second phase of the coding in grounded theory is described Figure 8.

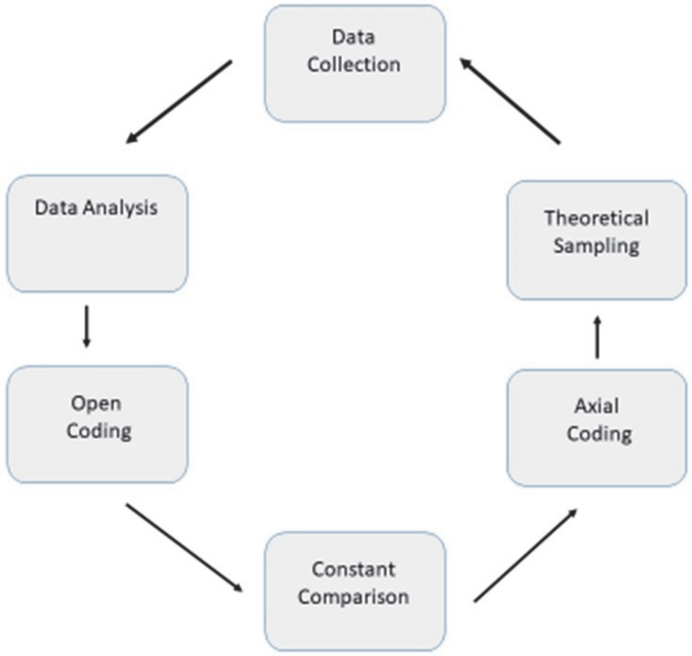


FIGURE 8 The first and the second phases of the coding in grounded theory

During the axial coding, the data collection continues. The focus of the data collection at this stage is to identify and test relationships between concepts and categories of open coding. Continuous comparison and questions guide the researcher in collecting data (Strauss & Corbin, 1990). The theoretical sample means additional material to be acquired that is relevant to the evolving theory. Complementary data collection continues until the theoretical saturation point is achieved. Theoretical saturation means that no more material can be found that could generate new categories, attributes or dimensions or new information in existing categories. In saturation, data analysis returns only codes that fit into existing categories. Each category is so developed that new or relevant material is no longer present. In the theoretical saturation, the ratio of the category to the other categories is well defined (Strauss & Corbin, 1998).

2.3.3 Selective Coding

In the third phase of the coding, selective coding, the categories are integrated and grouped around and connected with the core category. Selective coding is the core process that converts the collected and categorized data into a model, pattern or system, consisting of groups of logically interrelated concepts (Birks & Mills, 2015). A pattern, model, is a collection of ideas that explains the subject and a set of arguments describing the subject (Dey, 1999). All three phases of the coding of grounded theory are presented in Figure 9. The phases should not be understood as a straightforward path model or as separate phases, but rather they are different ways to handle material.

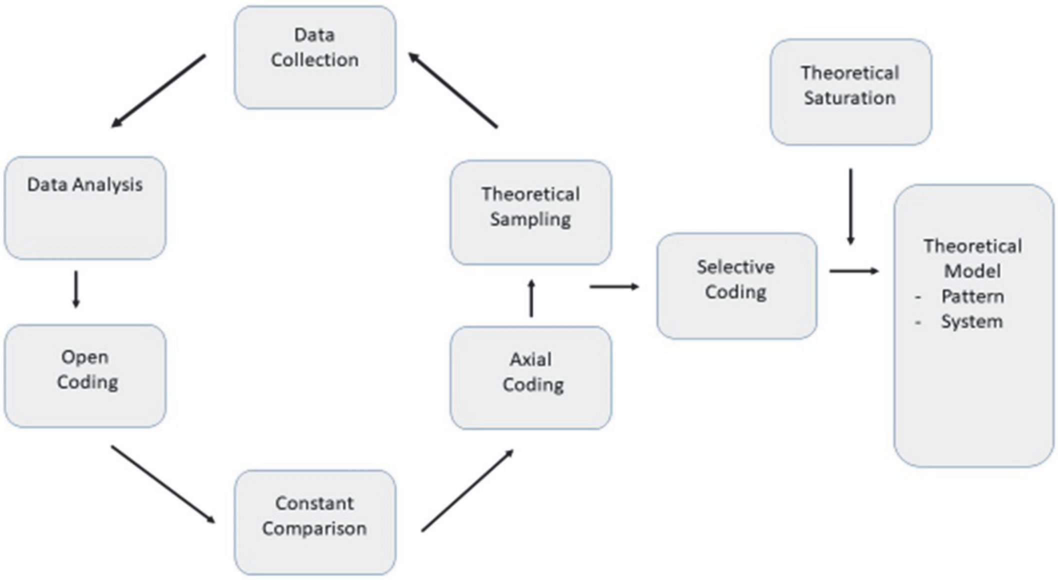


FIGURE 9 Three phases of the coding of grounded theory

The research question is a statement which identifies the topic under discussion and tells the reader which particular topic the researcher is interested in (Strauss & Corbin, 2008). It tells where the researcher wants to concentrate and what he wants to know about the topic being studied. The research question is often directed at the activity and processes of the phenomenon or subject being studied. The original research question is an instruction that gets the researcher to start, leads the researcher to the data and helps the researcher to focus on the essential throughout the study.

Selective coding means the integration of categories around the core category. The core category should account for the variation found in the data, that is, the categories will relate to it in some way. In selective coding is examined the relationship between the core category and other categories and is selected for construction of the pattern of those categories, whose linkage is possible to demonstrate clearly. A pattern, a story, or both can be used to describe the whole. (Strauss & Corbin, 1998)

A simple grouping of concepts under more abstract headings does not form a category. A category must be developed through the relationships of features and dimensional phenomena, through the action and interaction by which it is expressed and through the consequences caused by these actions. Questions to clarify the features of category could be as follows: What are the concepts belonging to this category? What manifestations does it have? What performance does it require? (Strauss & Corbin, 1990) In selective coding, the coding of factors that can naturally be linked to this main category begins.

Grounded theory's data collection differs from traditional data collection, where the researcher collects the material before the beginning of the analysis phase. Issues and questions related to concepts guide the next data collection round. In grounded theory, the collection of data leads to analysis, while analysis again leads to the formation of concepts. The concepts give rise to questions, which, in turn, guide the data collection.

In selective coding, the data collection is targeted. Data is selected from the collection, which will increase the opportunities to strengthen the story needed to produce theory, fortify relationships between the categories, and enhance poorly developed categories. It is also important to collect data which conflict with the researcher's own thinking and pattern under development. This does not necessarily prove the inaccuracy of the researcher's thinking and story, but offers an alternative and needed variation. By tracing the circumstances behind the data conflicting with the developed pattern and views, in the best case, it might be possible to make conclusions which support the researcher's own views and opinions (Strauss & Corbin, 1990).

The collection should be continued until the theoretical saturation of each category is reached. Theoretical saturation means that all concepts are defined with sufficient precision and new concepts are no longer found. If the theoretical sampling is terminated before saturation, the data remain conceptually insufficient (Corbin & Strauss, 1990). Once the core category has been found and selected, the theoretical collection is targeted to create and collect data, which saturates the core category and related categories and sub-categories (Birks & Mills, 2015).

2.3.4 Grounding the Model

The grounding of the model begins during the coding process. In grounded theory, this model means a pattern or system consisting of groups of logically interrelated concepts (Birks & Mills, 2015). The model means new structured knowledge of a system, consisting of groups of logically interrelated concepts and providing understanding and situation awareness. The model is a collection of ideas that explain the subject and a set of arguments describing the subject (Dey, 1999). The model can therefore both explain and predict the phenomenon to be studied. According to Glaser and Strauss (1967), the aims of grounding the theory are as follows:

- predicting and explaining the behaviour of the subject being investigated
- production of practical applications—the prediction and explanation should give the practitioners understanding and situation awareness
- providing a point of view on the behaviour of the subject
- providing a certain type of research related to the subject's behaviour

In axial coding, certain recurring relationships and dependencies between concepts and categories are discovered. At this stage, it is important to identify the recurrences and patterns and group the material accordingly (Corbin, 2008). In selective coding, categories are bound around the core category by a paradigm. The story of the central phenomenon is coded and presented analytically. The story is a description of the main phenomena of the study. It must not be isolated from the data. The story should start to emerge early in the research when the continuous comparison begins (Birks & Mills, 2015).

The story has two tasks. It integrates and explains the interdependencies between categories. The use of the story reveals the gaps and shortcomings in the data and analysis. Gaps force the researcher to return to the data and data collection (Birks & Mills, 2015). The story is used as a guideline, and the categories are reorganized and re-paradigmed until the categories seem to be appropriate to the story. When the categories match the story, an analytic version of the story is produced (Corbin, 2008).

2.4 Theoretical Sensitivity

Theoretical sensitivity refers to an individual's personal quality as a researcher. Theoretical sensitivity means the researcher's ability to identify what pieces of the data are relevant to the research, to give meaning to these pieces and to perceive the dimensions of the data. Theoretical sensitivity can be developed by reading both research literature and research data. Personal experience is also a source of theoretical sensitivity. For example, a divorcee is likely to better identify issues of in material on divorces.

A basic understanding and knowledge of the phenomenon being studied is vital because analysis is based on the induction and intuition of the researcher. Theoretical sensitivity also means the ability to maintain a balance between creativity and science (Strauss & Corbin, 1990).

In addition, professional experience helps to better understand the context and can increase the theoretical sensitivity. Data collection and comparison of the data, started before the analysis phase, generate small theoretical frames of concepts and their relationships (Strauss & Corbin, 1990).

The researcher brings to the analysis of his data his prediction and bias, his thinking, knowledge, and experience. These can prevent the researcher from seeing what pieces of the data are relevant. At the same time, they prevent the researcher from moving to analysis from a descriptive, from a working model describing subject and phenomenon.

The methods and techniques used in grounded theory to prevent prejudices and thinking from influencing the analysis include, for example, continuous questioning, analysis of an individual word and sentence, and continuous comparison. The phenomenon should also be viewed through the phenomenon's own cultural perspective and, for example, its own operational perspective, not through the perspective of researcher (Strauss & Corbin, 1990).

2.5 Grounded Theory and Quality of Research

The quality of research carried out by grounded theory is influenced by the researcher's expertise, methodological consistency (methodological congruence) and procedural precision. According to Corbin and Strauss (2008), a number of researchers' personal qualities, such as motivation, commitment, clarity of purpose, and self-awareness, improve the quality of the research. Characteristics of a good researcher include scientific accuracy, analyticity, sensitivity to the source data, and the ability to maintain a certain distance between the material and researcher's initial assumptions (Strauss & Corbin, 1998).

According to Birks and Mills (2015, 34), the researcher's expertise includes competence in scientific writing, the ability to find source material, and the ability to handle the research and writing process. Methodological consistency is the basis of reliable and credible qualitative research. Consistency is achieved when the researcher's personal attitude, the goals of the research and the research method used are consistent. In this thesis, the following key principles and practices were followed:

- wide and flexible definition of research questions
- data-based study
- careful reading of source material
- making notes
- extending the source material collection
- theoretical saturation
- parallelism of collecting and analysing the data
- continuous comparison
- progress of the analysis in three phases

Although one of the principles of grounded theory is continuous comparison, the researcher should "step back from the data" from time to time and ask if the emerging picture correlates with the reality of the data. The researcher must maintain a sceptical attitude to the data, the subject and the methods. All the theoretical explanations, categories, and hypotheses, directly or indirectly by comparison, either from the literature or from experience should be considered temporary. They should always be checked and compared with actual data. They should never be considered directly as facts (Strauss & Corbin, 1990). In this thesis, the period of research (more than three years) and the pauses caused by other work in the research has forced the author of this thesis to "step back from the data" a number of times.

3 DATA AND DATA ANALYSIS

3.1 Used Data

The primary data of this thesis consist of Russian official documentation. These include strategies, doctrines, laws, drafts of laws, presidential and governmental decrees, directives and planning, and guidance documents from different state agencies and organizations working in the area of information security. The most important of these agencies and organizations are the Federation Security Service (FSB), the Federal Service for Technical and Export Control (FSTEC), and the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor).

These documents can be considered as reliable valid primary sources, because the Russian state authorities use them to describe and explain the cyber threat to Russian society and people, and to help guide them in countering cyber threats. These documents include information close enough to the real picture to give as accurate information as possible on countering cyber threats.

According to the law on strategic planning of the Russian Federation (FZ-172, 2014), the hierarchy of Russian official documents for strategic planning in the area of cyber security management includes the following documents:

- Annual speech of the president to the Federal Assembly
- Strategy for the Development of an Information Society in the RF 2017-2030
- National Security Strategy
- Main Directions and Bases of Politics
- Doctrines
- Other records and documents

The Russian Federation President's annual address to the Federal Assembly is the guideline for strategic planning in Russia (FZ-172, 2014). In December 2016, Putin (2016) stated in his annual address that digital technologies include risks, and that is why Russia must strengthen its defense against cyber threats and make all the elements of its infrastructure, financial system, and state leadership and management more stable.

The Strategy for the Development of an Information Society in the Russian Federation 2017-2030 (UP-203, 2017) defines the aims, tasks and means of foreign and internal policy of Russia related to the use of information and communication technology (ICT) to develop an information society, create a national digital economy, and support national interests and strategic national priorities.

The National Security Strategy of the Russian Federation (UP-683, 2015) defines Russia's national interests, strategic priorities, objectives, tasks, and measures in domestic and foreign policy, which are aimed at strengthening the national security and ensuring Russia's sustainable development in the long term.

The Foreign Policy Concept of the Russian Federation (UP-640, 2016) includes basic principles, priority areas, goals and objectives of Russian foreign policy. The aim of the Foreign Policy Concept is to ensure national security, sovereignty, and territorial integrity and to consolidate Russia's position as a centre of influence in today's world.

The most important subject-related doctrines are the Military Doctrine of Russia (MDRF, 2014) and the Information Security Doctrine of Russia (UP-646, 2016), hereinafter IS Doctrine 2016. The Military Doctrine 2014 contains official views on the nature of conflict, the threat posed to Russia and on the use of force against these threats. The Military Doctrine 2014 establishes a framework for the Information Security Doctrine, both of which discuss the paradigm and strategic preferences in the cyber environment.

The IS Doctrine 2016 (UP-646, 2016) constitutes official views on ensuring Russian national security in the information space. The IS Doctrine 2016 includes descriptions of the information space as well as Russia's national interests and the threats it faces in the information space. The strategic preferences of Russian cyber security management are discussed in the doctrine.

Other documents dealing with cyber threat perception and cyber security management include subject-related laws, decrees, executive orders and other legislative documents and normative and methodological documents (Lapina, Revin and Lapin, 2004; Komarov, 2016). The subject-related laws and other legislative documents include the following:

- International information security agreements made by the Russian Federation
- Constitution of the Russian Federation
- Legislation of the Russian Federation
- Decrees of the President of the Russian Federation
- Decisions and orders of the Russian Federation Government

A Decree of the President of the Russian Federation, as a normative legal act, has the status of a by-law in the hierarchy of legal acts. A by-law is a rule or law established by an organization or community to regulate itself, as allowed or provided for by some higher authority. The Government of Russia can issue decisions and orders. Presidential decrees and governmental decisions and orders may not alter existing laws of higher precedence. Normative and methodological documents on the cyber threat and cyber security management include the following:

- Documents of the Security Council of Russia
- Documents of the Federation Security Service (FSB)
- Documents of the Russian Technical and Export Controls Federation Service (FSTEC)
- Legal norms of the Russian Federation Ministries and Administrations
- State Standards of the Russian Federation

The Security Council of Russia drafts policy proposals on defending the interests of Russia against internal and external threats. The council helps determine the security policy of the Russian Federation. Agencies such as the Federation Security Service (FSB) and the Federal Service for Technical and Export Control (FSTEC) may enact regulations through their general competency (UP-569, 2017). These documents, usually orders and instructions, are limited to the extent of the constitution and relevant codes.

The FSB is the principal security agency of the Russian Federation. Its primary functions and roles include law enforcement, counterintelligence, counterterrorism, and fighting against especially dangerous forms of crime domestic surveillance, and internal intelligence functions at the national level. Cyber and Internet surveillance is a new focus of collective FSB signal intelligence (SIGINT) efforts (UP-799, 2006).

The FSTEC is a federal executive authority implementing national policy, and exercising special and control functions in the sphere of state security in the areas of information security in information and telecommunication infrastructure systems. The tasks of the FSTEC also include countermeasures against foreign technical intelligence in the territory of the RF, the protection of sensitive information, and export control (UP-1085, 2004).

Secondary sources include official press releases, newspaper articles, and online materials from Russian news agencies. The blogs and webpages of Russian information security specialists have also been used as secondary sources because of the commentaries and discussions, which have clarified some of the ideas and aspirations of the Russian authorities behind the official language used in laws and other documents.

Data collection for this research began in 2015. Data collection was continuous and constant process, because the authorities of the Russian Federation were and still are publishing continuously and constantly official documentation on cyber threat and cyber security management. During the collection the new data were constantly compared with the material already analysed to find similarities and differences between concepts and categories. More than 140 official documents were collected and then coded.

3.2 Application of Grounded Theory in Data Analysis

3.2.1 Coding Process in Practice

The data collection for this thesis started in 2015. Atlas.ti[2] was used for the coding of the data. During the coding, more than two thousand concepts, categories and definitions were found, coded and compiled to tables, showing the interconnections between the concepts. The data were coded and compiled into tables twice. the first time was to verify that the tabular format was a logical and practical way to build the structural model of Russian cyber threat perception and Russia's response to the cyber threat, and verify that the concepts and the categories in the tables are accurate. Table 1 presents an extract of a table showing interconnections between the concepts and categories.

TABLE 1 Extract of a table showing interconnections between the concepts and categories

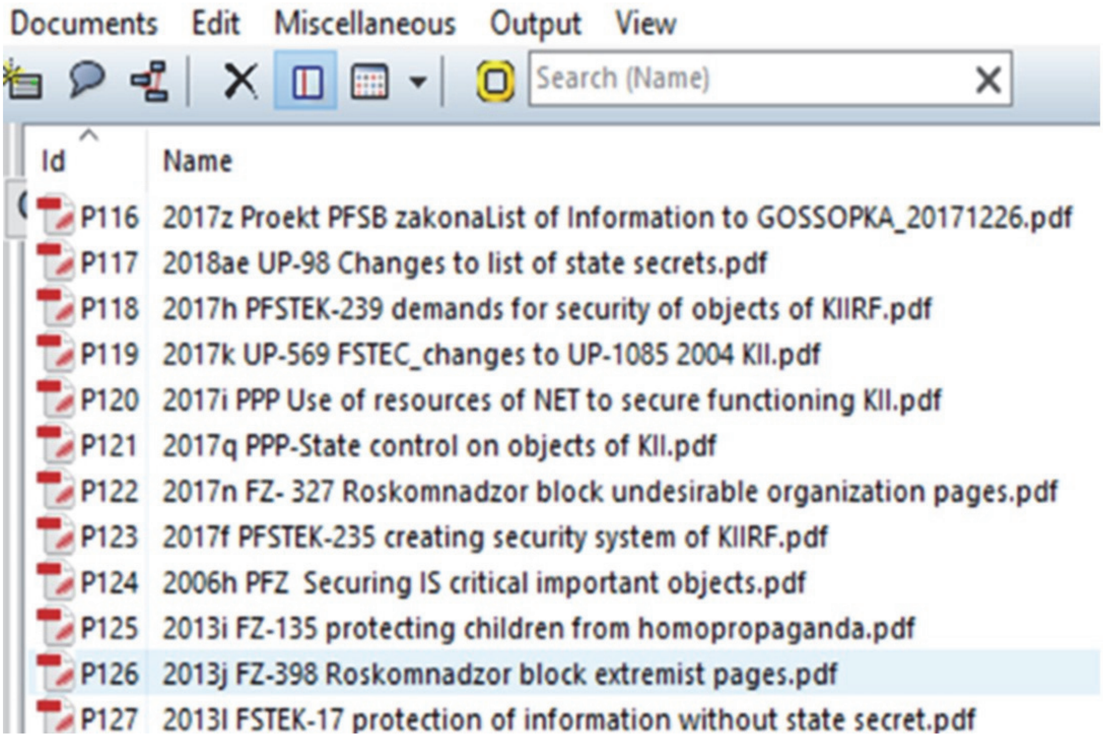
TS – Subject of threat	TT – Object of cyber threat	DM - Means of cyber threat
Unequal division of Internet resources	Stable and safe functioning of the Internet	
Foreign states Information terrorism Cyber crime Harmful natural phenomena	Information infrastructure, its objects and stable functions Telecom-operators Russia's critical information infrastructure, its components and functions	Development and use of information weapons Preparations for information war Malware Cyber-attack Cyber intelligence Capability for cyber-attacks Breach of information security
Foreign states Terrorists Terrorist organizations Extremist movements	Information telecommunication networks and their automated control systems and their functioning Special communication networks	Cyber-attack Cyber intelligence Cyber malfunction Disturbance of ICT systems Monopoly of software production Exploitation of dominant position in information space

[2] Jyväskylä University (JYU) has purchased Atlas.ti licenses for the students and the use of Atlas.ti is both supported and trained by JYU

Another reason to recode the data is that after the first tabulation at the end of 2016, a significant amount of new cyber security related documentation was published in Russia. In July 2016, Russian parliament approved the so-called Yarovaya laws (FZ-374, 2016, FZ-375, 2016), which included an expansion of authority for law enforcement agencies, new requirements for data collection and mandatory deciphering in the telecommunications industry. A new Russian information doctrine was published in December 2016 (UP-646 2016) and the Law on security of CIIRF (FZ-187, 2017) in July 2017.

The draft of law (PZF 608767-7, 2018) which aims to improve Russian digital sovereignty by creating the technical and operational capability to isolate the Russian segment of Internet from the global Internet was in the process of being passed in the Duma in the winter of 2018–2019. This Federal Law on Amendments to the Federal Law on Communications and to the Federal Law on Information, Information Technologies and Information Protection was signed by President Putin at the beginning of May 2019.

The third reason for recoding the data was because the thesis discussed not only cyber threat perception but also the response to that threat. This meant that the data which had coded been earlier for my master's thesis but only for threat perception, had to be recoded. The application of grounded theory in data analysis started with the collection of documents. Official documents were collected to Atlas.ti from the website of the corresponding ministry, agency, or other state organs. Figure 10 presents an extract of the list of documents in Atlas.ti.



Id	Name
P116	2017z Proekt PFSB zakonaList of Information to GOSSOPKA_20171226.pdf
P117	2018ae UP-98 Changes to list of state secrets.pdf
P118	2017h PFSTEK-239 demands for security of objects of KIIRF.pdf
P119	2017k UP-569 FSTEC_changes to UP-1085 2004 KII.pdf
P120	2017i PPP Use of resources of NET to secure functioning KII.pdf
P121	2017q PPP-State control on objects of KII.pdf
P122	2017n FZ- 327 Roskomnadzor block undesirable organization pages.pdf
P123	2017f PFSTEK-235 creating security system of KIIRF.pdf
P124	2006h PFZ Securing IS critical important objects.pdf
P125	2013i FZ-135 protecting children from homopropaganda.pdf
P126	2013j FZ-398 Roskomnadzor block extremist pages.pdf
P127	2013l FSTEK-17 protection of information without state secret.pdf

FIGURE 10 Part of the list of documents in Atlas.ti

3.2.2 Open Coding and Axial Coding

In open coding the documents were read line by line to find basic concepts related to the cyber threat and response to that threat and to define their features and dimensions. The lower-level concepts form the basis for the grouping of the higher-level concepts. The examples of the concepts found in the data of this thesis are critical information infrastructure of the Russian Federation, cyberspace attack and critical object of the information infrastructure.

The higher level concept information infrastructure of the Russian Federation includes, for example, lower-level concepts such as objects of information infrastructure and the telecommunication networks used to organize the interaction of these objects. The higher level concept cyberspace attack includes, for example, lower level concepts such as denial of service attack(DoS), decentralized denial of service denial attack (DDoS) and advanced persistent threat (APT) attack. More than two thousand words or combinations of words describing or defining lower or higher level concepts were found from the data.

In categorization, the concepts are grouped into categories, meaning groups based on the corresponding phenomenon. The categories of cyber threat which emerged from the data during open coding are as follows:

- objects (targets) of the cyber threat
- subjects (sources or factors) of the cyber threat
- Tactics, techniques and procedures (TTP) of the cyber threat
- consequences of the realized cyber threat

The categories of Russia's response to the cyber threat, that is, the categories of cyber defense emerging from the data, are the following:

- objects of cyber defense, targets of the cyber threat
- subjects of cyber defense, actors responding to the cyber threat
- Tactics, techniques and procedures (TTP) of cyber defense
- The aims of cyber defense
- limitations and problems of Russian cyber defense

The codes used for categorization of the concepts of Russian cyber threat perception are presented in Table 2. The codes used for categorization of the concepts of Russia's response to cyber threat are presented in Table 3. The names of categories emerged during the coding process. When, for example, a concept related to the object of cyber threat was found in the text for the first time, a new category was established, Object of Cyber Threat. After that, all other concepts related to the object of cyber threat, which were found later in the text, were also coded as Object of Cyber Threat. Defense TTP and Means of Cyber Defense, presented in Table 3, were coded separately at the beginning of process, but they were later merged because it was not always possible to separate means from tactics, techniques and procedures.

TABLE 2 Codes for categorization of the concepts of Russian cyber threat perception

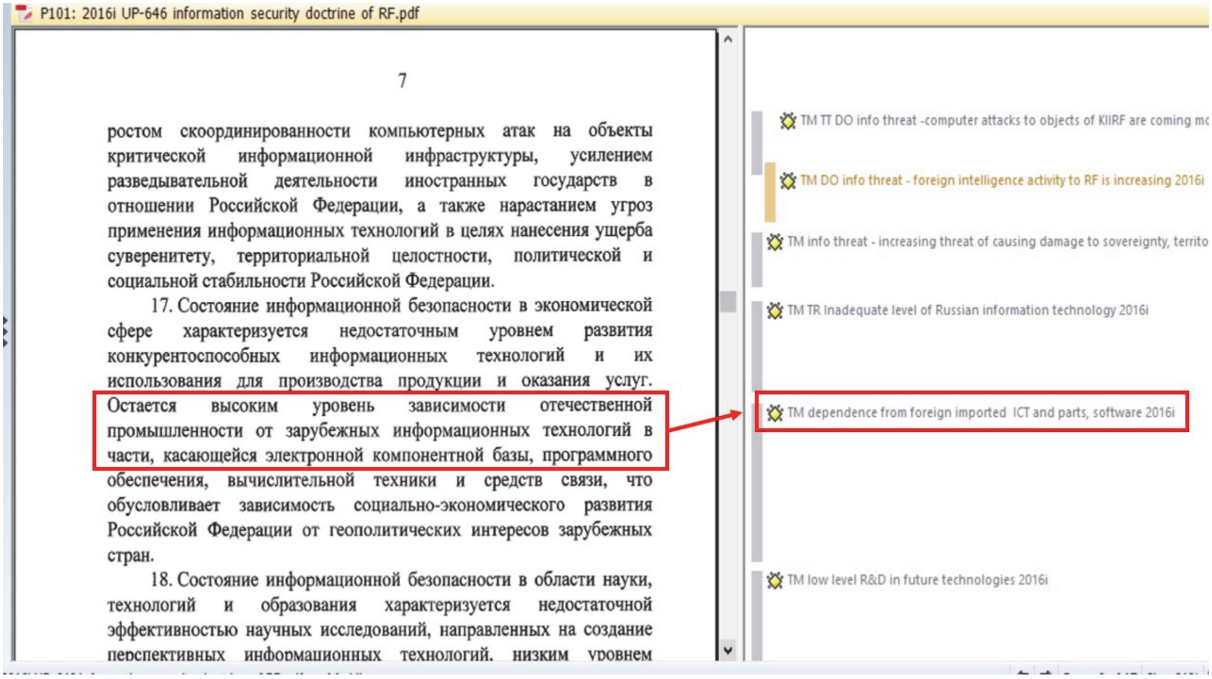
Code	Name of the Category	Meaning/Remarks
TT	Object of Cyber Threat	Targets of (cyber) Threat
TS	Subject of Cyber Threat	Threat Subject of the cyber threat
TM	Means of Cyber Threat	Threat Means, i.e. TTP used by an attacker
TR	Result of Cyber Threat	Consequences of the realized cyber threat

TABLE 3 Codes for categorization of the concepts of Russia's response to the cyber threat

Code	Name of the Category	Meaning/Remarks
DO	Object of Cyber Defense	Defense Objects (targets of the cyber threat)
DS	Subject of Cyber Defense	Defense Subject, responding to cyber threat
DT	Defense TTP	Defense Tactics, i.e. TTP used by defender
DM	Means of Cyber Defense	Defense Means, i.e. TTP used by attacker
DA	Aim of Cyber Defense	Defense Aims, operative goals of defense
DL	Limitation to Cyber Defense	Limitations of Russian cyber defense

Example of the conceptualization and categorization of open coding process by using Atlas.ti is in Figure 11. A part of the text of the Information Security Doctrine 2016 (UP-646, 2016) discussing computer attacks on Critical Information Infrastructure of the Russian Federation has been found in the text, and marked green. Then this part of the text has been coded. The codes assigned to this text are means of cyber threat (TM), as Object of Cyber Threat (TT) and Object of Cyber Defense (DO). After the codes, I written a short description: "computer attacks to objects of KIIRF are becoming more complicated and frequent and more coordinated 2016i", where 2016i is the code for the Information Security Doctrine 2016 (UP-646, 2016).

As a result of the conceptualization and categorization process a list of categorized concepts of the Russian cyber threat perception and response to that threat was established. Figure 12 presents an extract of the list. The list was used in axial coding to create connections and links between the concepts and categories created in open coding. Axial coding identified the core category, which represents the main theme of this study and has the greatest explanatory relevance and highest potential for linking other categories together. The core category of this research is Object of Cyber Threat.



P101: 2016i UP-646 information security doctrine of RF.pdf

7

ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.

17. Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.

18. Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем

TM TT DO info threat -computer attacks to objects of KIIRF are coming mc

TM DO info threat - foreign intelligence activity to RF is increasing 2016i

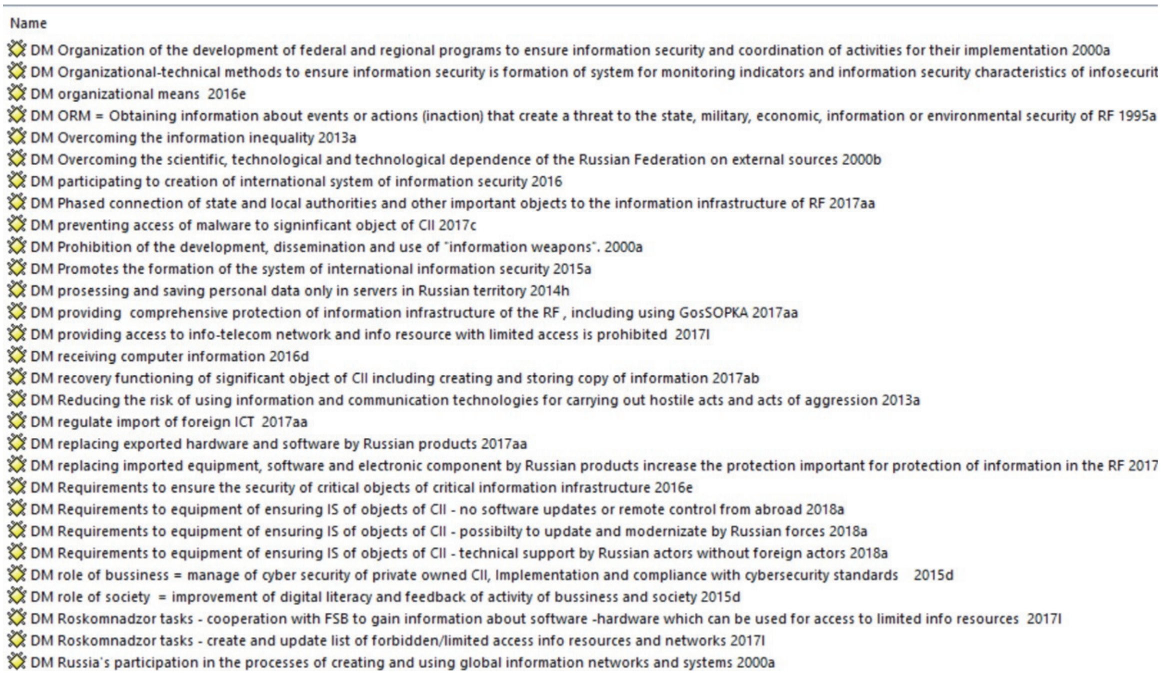
TM info threat - increasing threat of causing damage to sovereignty, territo

TM TR Inadequate level of Russian information technology 2016i

TM dependence from foreign imported ICT and parts, software 2016i

TM low level R&D in future technologies 2016i

FIGURE 11 Example of conceptualization and categorization process of the Information Security Doctrine (UP-646, 2016) by Atlas.ti



Name

DM Organization of the development of federal and regional programs to ensure information security and coordination of activities for their implementation 2000a
DM Organizational-technical methods to ensure information security is formation of system for monitoring indicators and information security characteristics of infosecurit
DM organizational means 2016e
DM ORM = Obtaining information about events or actions (inaction) that create a threat to the state, military, economic, information or environmental security of RF 1995a
DM Overcoming the information inequality 2013a
DM Overcoming the scientific, technological and technological dependence of the Russian Federation on external sources 2000b
DM participating to creation of international system of information security 2016
DM Phased connection of state and local authorities and other important objects to the information infrastructure of RF 2017aa
DM preventing access of malware to signinficant object of CII 2017c
DM Prohibition of the development, dissemination and use of "information weapons". 2000a
DM Promotes the formation of the system of international information security 2015a
DM prosessing and saving personal data only in servers in Russian territory 2014h
DM providing comprehensive protection of information infrastructure of the RF , including using GosSOPKA 2017aa
DM providing access to info-telecom network and info resource with limited access is prohibited 2017l
DM receiving computer information 2016d
DM recovery functioning of significant object of CII including creating and storing copy of information 2017ab
DM Reducing the risk of using information and communication technologies for carrying out hostile acts and acts of aggression 2013a
DM regulate import of foreign ICT 2017aa
DM replacing exported hardware and software by Russian products 2017aa
DM replacing imported equipment, software and electronic component by Russian products increase the protection important for protection of information in the RF 2017
DM Requirements to ensure the security of critical objects of critical information infrastructure 2016e
DM Requirements to equipment of ensuring IS of objects of CII - no software updates or remote control from abroad 2018a
DM Requirements to equipment of ensuring IS of objects of CII - possibilty to update and modernizate by Russian forces 2018a
DM Requirements to equipment of ensuring IS of objects of CII - technical support by Russian actors without foreign actors 2018a
DM role of bussiness = manage of cyber security of private owned CII, Implementation and compliance with cybersecurity standards 2015d
DM role of society = improvement of digital literacy and feedback of activity of bussiness and society 2015d
DM Roskomnadzor tasks - cooperation with FSB to gain information about software -hardware which can be used for access to limited info resources 2017l
DM Roskomnadzor tasks - create and update list of forbidden/limited access info resources and networks 2017l
DM Russia's participation in the processes of creating and using global information networks and systems 2000a

FIGURE 12 An extract of the list of categorized concepts of Russian cyber threat perception and the response to that threat

3.2.3 Selective Coding

In selective coding, the categories were integrated and grouped around and connected with the core category, Object of Cyber Threat. The aim of selective coding was to answer the three research questions:

- What is Russia's cyber threat perception?
- What are the most important objects to protect in Russia's cyber threat perception?
- How is Russia responding to cyber threats?

According to Dey (2001), pattern, or model, is a collection of ideas that explain the subject and a set of arguments describing the subject. This means searching the story line, the core category of the research, to which other categories will be associated. In selective coding, the relationship between the core category, Object of Cyber Threat, and other categories was defined and selected for construction of the story used to describe the phenomenon.

The categories were developed, according to guidance of Corbin and Strauss (1990), on the basis of the relationships between features and the action and interaction as well as on the consequences caused by these actions. For example, when a category, such as Object of Cyber Threat, was created and this category was identified in the data, there was a need to clarify some of the features related to this category. Questions to clarify the features of category Object of Cyber Threat could be, for example: What are the concepts belonging to this category? What manifestations does it have? What performance does it require? In selective coding, the coding of factors that can naturally be linked to this main category is initiated. In selective coding, the data collection was targeted. The core category, Object of Cyber Threat, emerged in the early phase of the research, which helped to guide the data collection.

3.2.4 Grounding the Model

At the fourth phase of application of grounded theory as method for data analysis the model of Russian cyber threat perception and threat response was constructed. The categories were bound around the core category, and the story of the central phenomenon started to emerge. The story integrates and explains the interdependencies between categories. The story was used as a guideline to reorganize the categories until they were appropriate to the story and an analytic version of the story, that is, a model of Russian cyber threat perception and response to that threat, was produced. In the story the attacker, meaning the subject of the cyber threat, tries to influence the object of the cyber threat using Tactics, Techniques and Procedures (TTP). The defender, meaning the subject of cyber defense, tries to defend the object of cyber defense using Tactics, Techniques and Procedures (TTP).

According to Glaser and Strauss (1967), a model can explain or predict phenomenon to be studied. In this thesis, the model provides understanding and situation awareness and a point of view on the behaviour, in this case, Russia's response to the cyber threat, and describes the Russian cyber threat perception by discussing the following:

- objects and subjects of the cyber threat to Russia
- objects and subjects of Russian cyber defense
- tactics, techniques and procedures (TTP) of the subject of cyber threat to Russia
- tactics, techniques and procedures (TTP) of the subject of Russia's cyber defense
- aims and limitations of Russian cyber defense

In this model, the subject of cyber threat means an actor who causes a threat to Russia in or through cyberspace. Objects of cyber threat are the targets that are by the subject of cyber threat. These objects of cyber threat are also objects of Russia's cyber defense, protected and defended by the actor of Russia's response to this threat, that is, by the subject of Russian cyber defense. TTP in this model means the tactics, techniques and procedures used by the subjects of cyber threat to Russia and by Russian cyber defense. The limitations of cyber threat refers to technical, operational and other limitations which prevent or complicate the Russian response to cyber threats. The aims of Russian cyber threat refer to strategic level aims related to cyber defense. Figure 13 presents the model of Russian cyber threat perception (red in the figure) and the response to that threat (blue in the figure).

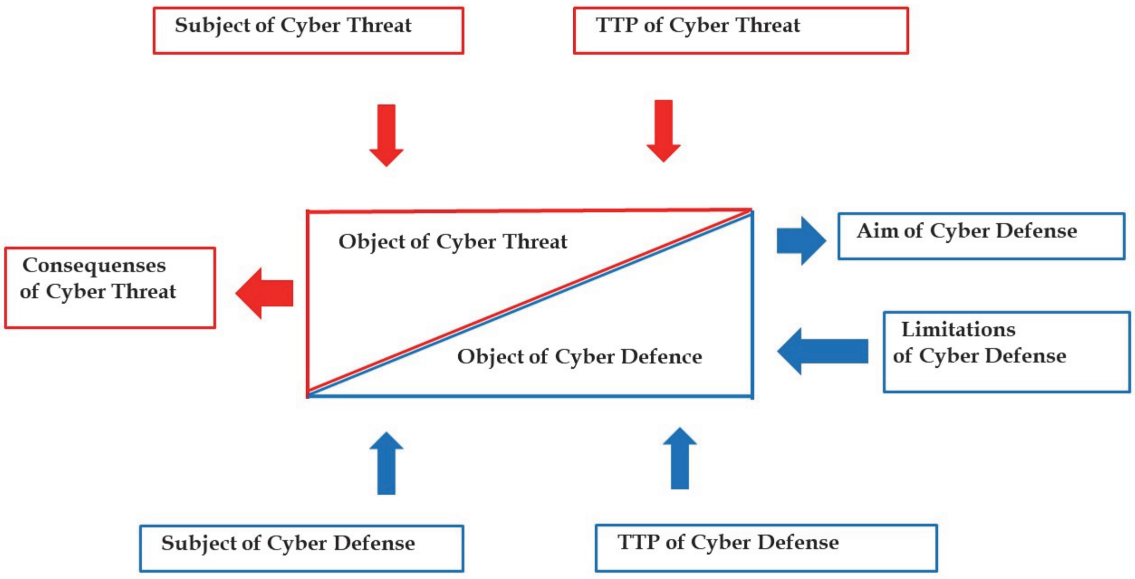


FIGURE 13 The model of Russian cyber threat perception and response to that threat

During the coding process, the category Object of Cyber Threat emerged as the core category. Lower level concepts belonging to the category of Object of Cyber Threat structured four higher level concepts: Russian National Interests in Cyberspace, Information Infrastructure, Information, and the Russian Armed Forces. The latter was studied as its own high-level concept, even though the targets inside Armed Forces are related either to information infrastructure or information and, in many cases, also to Russian National Interests in Cyberspace. This is because issues related to the Armed Forces, both in cyber threat perception and their response, were typically discussed in documents that were separate from the other issues.

The division into these high-level concepts is partly artificial, and the concepts overlap each other. For example, information is typically stored, processed or transmitted in information infrastructure. The division was used first to guide the data collection and then to parse and to structure the phenomenon.

This model guided not only the data collection, but whole the study. The results are presented next, in Chapter 4. The model also creates the starting point and material for the research question: "How does Russian strategic culture explain Russia's cyber threat perception and the response to that threat?" This question is discussed in Chapter 5.

4 RUSSIAN CYBER THREAT PERCEPTION AND RESPONSE TO CYBER THREATS

4.1 Russian Cyber Threat Perception

During the data analysis, described in Chapter 3, Object of Cyber Threat emerged as the core category, from which four higher-level concepts emerged. These concepts are Russian national interests in cyberspace, information infrastructure, information, and Russian Armed Forces. Article I, "Russia: A Cyber Fortress Besieged," written in early spring 2017, presents a fifth concept, Other Targets of Cyber Threat, including for example electrical grids and the functioning of nuclear power plants and chemical and medical industries. This categorization was changed after the passage of the Law on Security of Critical Information Infrastructure of the Russian Federation (ZF-187, 2017), herein after CII Security Law, in July 2017. The CII Security Law clarified the situation by defining that most of these objects, which were categorized in the first article in Other Targets of Cyber Threats are part of the critical information infrastructure, and belong to the higher-level concept Information Infrastructure.

The four higher-level concepts partly overlap each other. For example, a cyberspace attack through information infrastructure on information can influence the Russian Armed Forces and Russian national interests. Despite this partial overlapping, the division of objects of cyber threat to these four higher-level concepts is used as the framework of this thesis. This conceptualization was sufficiently clear and well defined to support both data collection and analysis, and serves as the framework for presenting the results of analysis. This chapter discusses, based on this conceptualization, first the objects and subjects of cyber threats, then technological arrearage of Russia and finally Russia's ways to respond to cyber threats.

4.1.1 Russia´s National Interests in Cyberspace

The first higher level concept of the core category is Russia's national interests in cyberspace. These interests include the inviolability of Russia's constitutional order, sovereignty, independence, political stability, national and territorial integrity (UP-640, 2016). Russia's national interests can be threatened in or through cyberspace by external or internal subjects, which can be Western states, extremists, terrorists and criminals. The penetration of foreign intelligence and special services into Russian information networks is an interference in Russia's internal affairs and can damage political stability. Terrorist organizations and extremists can also conduct cyber-attacks on Russian targets, in this manner threatening Russian national interests (UP-24 2000; MDRF, 2014; UP-683, 2015; SBRF, 2016).

In strategic level, the cyber threat to Russia is part of the wider threat to Russia´s strategic interests. The use of the Stuxnet malware against Iranian nuclear facilities was the first example of new generation warfare and showed that cyber weapon will at least partly be the "weapon of the century". A similar attack, as Stuxnet attack was, on Russian targets could cause enormous damage to Russia's economy if it could not be countered (Orlov, 2011).

4.1.2 Information Infrastructure

The second higher level concept of is information infrastructure. The information infrastructure of the Russian Federation is defined in the Information Security Doctrine 2016 (UP-646, 2016) as

> A complex of objects of informatization, information systems, sites on the Internet, and communication networks, which are located in the territory of the Russian Federation and in the territories under jurisdiction of the Russian Federation or used as the bases of international agreements of the Russian Federation. [3]

The information infrastructure of the Russian Federation includes critical information infrastructure, its components and functions, information telecommunication networks and their automated control systems, special communication networks, telecom operators, and information processing and information security (IS) management technology. The information processing and IS management technology includes software, hardware, operating systems, encryption keys and cryptographic protection systems (FZ-40, 1995; UP-334, 1995; FZ-5, 1996; UP-24, 2000; FZ-152, 2006; MDRF, 2011; FZ-1, 2013; UP-31, 2013; SBRF, 2012; SBRF, 2013; RBA, 2013; RCA, 2015; SBRF 2016; UP-646, 2016).

According to the Russian assessment, the exploitation of cyberspace (espionage) and the possibility of cyberspace attacks on the Russian information infrastructure have increased. Cyberspace attacks against the critical information infrastructure are becoming more complex, more frequent, and more coordi-

[3] UP-646, 2016

nated (UP-646, 2016), and these attacks can have a destructive impact on the infrastructure. Internal enemies such as terrorists and extremists are among those creating the means to have this kind of destructive impact (UP-203, 2017). These threats can result in a loss of control, the destruction of infrastructure, irreversible negative change (or destruction) of the economy of the country or an administrative-territorial unit or a significant, long-term deterioration in the safety of the population living in these territories. This all causes a sense of vulnerability in Russian leadership. (see FZ-5, 1996; UP-24, 2000; FZ-152, 2006; MDRF, 2011; FZ-1, 2013; UP-31, 2013; SBRF, 2012; SBRF, 2013; RBA, 2013; RCA, 2015; SBRF, 2016; UP-646, 2016)

Permanent war against Russian digital sovereignty is waged every day (Sinovets, 2016). According to Nikolai Murashov, the Deputy Director of the National Computer Incident Coordination Center, more than four billion computer attacks on Russian critical infrastructure were detected in 2018 by the State System for the Detection of Warnings and Elimination of Computer Attacks (GosSOPKA). More than 17,000 of the attacks were categorized as the most dangerous. In 2017, the number of computer attacks on Russian critical infrastructure was 2.5 billion, of which 12,300 were classified as the most dangerous (Interfax, 2018).

4.1.3 Information

Information is third higher level concept. The information resources of the Russian Federation consist of secret and confidential information (FZ-40, 1995; FZ-61, 1996), state secrets (FZ-4524, 1993; FZ-5485, 1993; FZ-40, 1995; FZ-61, 1996; SBRF, 2000; UP-646, 2016), business and service secrets (UP-188, 1997; FZ-149, 2006), personal and family secrets. Information resources also include information necessary for society, open information resources and personal data (FZ-152, 2006; SBRF, 2016).

The confidentiality, integrity and availability of information are targeted by the intelligence services of foreign states (SBRF 2000), terrorist organizations and cyber criminals (YA, 2009; SBRF, 2013; RBA, 2013; RCA, 2015). The tactics, technics and procedures of those violating Russian information resources include cyberspace attacks and cyberspace exploitation (cyberspace intelligence), including unauthorized intrusions into information systems to steal, manipulate, forge, change or destroy information or to block access to information. Concealment, delay in receipt, distortion, leakage and destruction of operational information are seen as threats to the information resources of the Russian Federation. Cyberattacks can be directed at the information saved in databases, processed in computers or transmitted in telecommunication networks (UP-24, 2000; YA, 2009; RBA, 2013; RCA, 2015). In addition, saving, processing and transmitting the information against regulations, technical malfunctions are mentioned as cyber threats (SBRF, 2011).

4.1.4 Armed Forces of the Russian Federation

The Armed Forces of the Russian Federation is the fourth higher level concept. Foreign special services, terrorist organizations, and extremist movements are targeting the information infrastructure, command and control structures and information resources of the Russian Armed Forces (MDRF, 2014). The main targets of possible cyberspace exploitation and attacks include strategic missile warning and defense systems, air and space defense forces, and strategic missile forces. The subject of the cyber threat, meaning the attacker, may try to weaken the defense capability of these strategically important systems and forces (SBRF, 2013; MDRF, 2014).

During a pre-war period and in the first phase of any hostilities, the mobilization of the Russian Armed Forces and the deployment of wartime troops to operational areas are potential targets of cyberspace attacks. The logistical systems supporting mobilization and strategic deployment would also be targets of cyberspace attacks before the outbreak of a war. The readiness of the Armed Forces is also targeted by foreign intelligence services in peacetime (FZ-61, 1996; YA, 2009; MDRF, 2010; SBRF, 2012; MDRF, 2014).

4.2 Technological Arrearage of the Russian Federation

One threat to Russia in cyberspace is the technological lag [4]of the Russian Federation in information and communication technology (ICT) from the leading foreign states. This gap limits Russia's capabilities to respond to cyber threats (PP-1895, 2000; UP-646, 2016). In 2013, Russia was estimated to be at least three to five years behind the USA in ICT development and production (Eliseev, 2013) and five-and-a-half years behind the USA in supercomputing technology (Moukin, 2013). This lag in the production, research and development of ICT has created a dependence on foreign information technology, which in turn has created a sense of vulnerability and weakened Russia's cyber defense, facilitates cyberspace intelligence operations in Russia and gives Western special services an opportunity to influence Russia's information resources (UP-683, 2015; SBRF, 2016; UP-646, 2016). In the draft of the Information Security Doctrine (PUP-1, 2015), this lag is recognized in the following statement:

> The state of information security of the Russian Federation in the economic sphere is characterized by the lag of the Russian Federation behind the leading foreign states in the development of competitive information technology, including supercomputers, and using them to create products and services based on them.[5]

[4] The Russian word used by Russians in Information Security Doctrine 2000 and in the draft of Information Security 2016 for the lag is отставание, which can also be translated as arrear, arrearage, gap and retardation.

[5] PUP-1, 2015

It is interesting to note that the reference to supercomputers and the comparison with the leading foreign states were deleted in the final version of the doctrine, in which the above sentence appeared as follows:

> The state of information security in the economic sphere is characterized by an insufficient level of development of competitive information technologies and their use for production and services.[6]

4.3 Russia's Response to Cyber Threats

4.3.1 Measures to Respond to Cyber Threats

Russia's measures to respond to cyber threats consist of interconnected juridical, organizational, intelligence, counter-intelligence, scientific-technical, informational-analytical, cadre, economic and other measures to predict, detect, contain, prevent and repulse information threats and to liquidate their consequences (UP-646, 2016).

These measures include Russia's aspiration to create and acquire a generally accepted international treaty or code of conduct to prevent the use of ICT for the violation of strategic stability and to protect the sovereignty of the Russian Federation in information space (UP-646, 2016). Cyber defense against external enemies and threats includes protection of critical information infrastructure and increasing digital sovereignty by improving the readiness and capabilities to isolate the Russian segment of the Internet from the global Internet. Data retention can also be considered a response to external cyber threats. The main measures of the Russian response to internal cyber threats are increased surveillance of the Russian segment of Internet, censorship, banning user anonymity and better user identification online. Russian state authorities and Armed Forces have their own special-purpose telecommunication networks that are totally or partly separated from Internet. Russia has also tried to develop his own ICT research, development and production partly as response to threat caused by the use of imported Western ICT.

4.3.2 Pivot to International Agreements on Cyber Security

Russia has tried to respond to cyber threats by entering into international or bilateral cyber security agreements and by drafting rules and codes of conduct which would prevent the use of information technology for military purposes or for terrorist, extremist or criminal purposes in cyberspace within the United Nations and the Shanghai Cooperation Organization. Established in June 2001, the Shanghai Cooperation Organization (SCO) is an intergovernmental organization comprising Kazakhstan, Kyrgyzstan, Russia, the People's Republic of China, Tajikistan and Uzbekistan. The SCO's main objectives are to strengthen mutual

[6] UP-646, 2016

trust and good neighbourhood relations, promote cooperation in the fields of politics, commerce, economy, science, technology and culture, and in education, tourism, energy and transport, and to develop and maintain peace, security and stability in the region (SCO, 2019).

In July 2009, at the Summit in Yekaterinburg, the CSO member states approved an agreement on cooperation in the field of international information security. The purpose of the Yekaterinburg Agreement is to limit international threats to information security, ensure the interests of the member states in information security and develop an international information space. The major threats to international cyber security are the development and use of cyber weapons and the preparation and implementation of cyber war, cyber terrorism, cybercrime, and using the dominant position in the information space of some states to produce harm and damage to other states (YA, 2009).

In a letter to the UN Secretary-General in January 2015 (UNGA, 2015), the SCO proposed acceptance of an International Code of Conduct for Information Security. The letter contains 13 rules of conduct that SCO wish to commit to other states. This Code of Conduct has not received much support, but it gives a good insight into Russia's view of the international legal regulation of the cyber environment.

The Code of Conduct notes, as was stated already in the Yekaterinburg Agreement, that Russia concerns that some states do not respect Russia's sovereignty but try to influence Russian internal affairs also in the cyberspace. The Code of Conduct states that online freedom may be restricted by legislation if it is necessary to protect national security, public order, or public health or morality (UNGA, 2015). That is why Russia is seeking international control of the Internet and an international agreement on information security. This means, for example, internationalization of critical internet management by transferring management of the Internet from ICANN to the ITU (Tsernenko & Demidov, 2015).

Information security has been on the agenda of the UN Office for Disarmament (UNODA) since 1998 by the proposal of the Russian Federation. Since 2004, the Group of Governmental Experts (GGE) has been working under UNODA, investigating cyber threats and measures to reduce them. During the fifth session of the UN Group of Governmental Experts' (GGE) in June 2017, disagreements emerged between Russia and the USA on the applicability of international humanitarian law and the right to self-defence in cyberspace. Russia proposed a resolution that consisted elements of a Code of Conduct of SCO, emphasizing sovereign rights for states to protect their information space against cyber threats. The GGE was not able to agree on a consensus report.

As a consequence of this disagreement, the United Nations General Assembly (UNGA) approved, in December 2018, the proposal of the Russian Federation to establish an Open-Ended Working Group (OEWG) in 2019 to develop the rules, norms and principles of responsible behaviour of states (UNGA, 2018b). UNGA also approved the creation of the next GGE, proposed by the USA (UNGA, 2018a). Russia is also attempting to respond to cyber threat also in future by creating international legal norms, which would prevent the use of information technology for military purposes or criminal or terrorist purposes within the United Nations and the SCO. Russia has plans to draft regulatory legal acts in international organizations concerning the sovereign right of states to determine information, technological and economic policies in the national segments of the Internet no later than March 2020 (APIS, 2017).

Russia has entered into an information security agreement with Belarus and China. In December 2013, Russia and Belarus signed an agreement on co-operation in maintaining international information security. The agreement describes threats to information space and then sets out common measures to combat threats. The list of threats in the agreement corresponds to the list in the Yekaterinburg Agreement (RBA, 2013). In April 2015, the Russian Federation and China signed a bilateral agreement on cooperation to maintain information security. Russia and China have agreed on measures to combat cyber threats and increase international information security (RCA, 2015). The measures are similar to those already agreed on by the countries in the Yekaterinburg Agreement in 2009. The agreement repeats the concerns expressed in the Yekaterinburg Agreement (YA, 2009) and the Code of Conduct (UNGA, 2015) about interference in Russia's internal affairs and the dissemination of harmful information.

According to Russia’s agreements with Belarus and China (RBA 2009; RCA, 2015), information space is threatened by the use of information communication technology for attacks that violate the sovereignty, security or territorial integrity of the state or threaten international peace, security or strategic balance or generating financial or other damage, including causing damage to information infrastructure. Other cyber threats include terrorism and offenses including illegal intrusion into computer information, interference in internal affairs, disruption of social order, destabilization of internal political and socioeconomic conditions, and damaging state leadership.

4.3.3 Protection of Critical Information Infrastructure

One of Russia’s interests in cyberspace is to ensure the sustainable and uninterrupted functioning of the Critical Information Infrastructure of the Russian Federation, CIIRF (UP-646, 2016). The Russian Information Security Doctrine, published in 2000, hereinafter IS Doctrine 2000, started to debate the protection of the CIIRF. The core question of this debate was the roles and responsibilities of different state authorities in IS management of the CIIRF. After publishing the IS Doctrine 2000, the protection of the CIIRF took almost two decades to be organized. The reason for the long debate was the power struggle over the division of the responsibilities between private companies and state organizations such as the Federation Security Service (FSB), the Federal Service for Technical and Export Control (FSTEC), the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor), and the Russian Armed Forces.

After two drafts laws for the security of the CIIRF (2006 and 2013), the State Duma finally passed the third draft version, CII Security Law, in July 2017 (FZ-

187, 2017). According to CII Security Law (FZ-187, 2017), the critical information infrastructure of the Russian Federation includes objects of critical information infrastructure as well as the telecommunication networks used to organize the interaction of these objects.

The objects of the CIIRF are information systems, information and telecommunication networks, and automatic control systems operating in the following sectors: defense, healthcare, transport, communications, credit and finance, energy and fuel, nuclear, rocket and aerospace, mining, metallurgical, and chemical. The threats to the CIIRF include unauthorized access, destruction, modification, blocking, copying, provision, and dissemination of information about an object of the CIIRF (FZ-187, 2017).

The protection of CIIRF is tasked to the Federation Security Service (FSB) and to the Federal Service for Technical and Export Control of the Russian Federation (FSTEC). The FSB operates the GosSOPKA, the state system for detecting, preventing and eliminating the consequences of computer attacks on the information resources of the Russian Federation (UP-620, 2017). The main task of GosSOPKA is ensuring the security of the information resources of Russia from computer attacks and maintaining the stable functioning of these resources in the face of incidents caused by computer attacks (SBRF, 2014; UP-620, 2017).

The FSB established and operates the National Coordination Center for Computer Incidents (NCCCI)[7], as well as regional and territorial information security operations centres (ISOC). The GosSOPKA ISOCs are to be established in the Russian Federation at the federal district[8] and subject[9] level. The ISOCs can be operated by the FSB, or they can be departmental or corporative ISOCs. At the administrative departmental level, a state body can establish a departmental ISOC[10] to protect the information resources of an administrative branch or department. State corporations, telecom operators and other organizations that carry out licensed activities in IS can establish and operate corporative ISOC to protect their own information resources.

The tasks of ISOCs include collecting and analysing information about computer attacks and computer incidents, responding to threats, and eliminating the consequences of computer incidents in information resources. (PFSB-366, 2018.) All the regional ISOC´s are planned to have full operational capability no later than in March 2024 (APIS, 2017).

The role of the FSTEC in the protection of the CIIRF is identification and categorization of the objects of the CIIRF and instructing the measures to protect categorized objects. Significant objects of the CIIRF are categorized into Category I, II or III, based on the social, political, economic, and environmental significance

[7] Национальный координационный центр по компьютерным инцидентам

[8] A federal district is a grouping of the federal subjects for the convenience of operation and governing by federal governmental agencies. There are eight federal districts in the Russian Federation.

[9] The subjects of the Russian Federation are the main administrative division in Russia. The federal subjects can be oblast, republic, krai, okrug, federal city or autonomous oblast

[10] ведомственный центр

or based on the significance for the country's defense, state security, and law and order. Category I is for the CIIRF's most significant objects.

After the categorization, the FSTEC provides requirements to ensure the security of categorized CIIRF objects and information and telecommunications networks and, in cooperation with the Ministry of Telecom and Mass Communications of the Russian Federation, includes them in the registry of significant CIIRF objects. For the banking and finance sector, the FSTEC sets requirements in consultation with the Central Bank of the Russian Federation. The subject of the CIIRF, meaning the owner or the user of the significant object of the CIIRF, is obliged to follow FSTEC instructions and establish security arrangements corresponding to the CIIRF object's category.

The FSTEC is authorized to evaluate the security arrangements of the objects included in the registry (FZ-187, 2017). The State Research and Testing Institute for Technical Information Protection Problems[11], which is part of the FSTEC, maintains a database of information security threats (PFSTEK-17, 2013). The database, which can be found at bdu.fstec.ru, was opened to public use in March 2015.

4.3.4 Improving Digital Sovereignty

The defense of Russia and the Soviet Union has traditionally been based on strong military and security organizations and on the pursuit of easily defended borders and buffer zones between any possible attacker and Russia's main territory. To secure digital sovereignty, Russia is planning to create easily defended borders in cyberspace by creating technical and operational readiness to disconnect the Russian segment of the Internet from the global Internet.

At the beginning of May 2019, President Putin signed a Law on Amendments to the Federal Law on Communications and on the Federal Law on Information, Information Technologies and Information Protection, herein after the RuNet Law (FZ-90, 2019). The aim of the RuNet Law is to improve Russia's digital sovereignty and to ensure the sustainable operation of the Russian segment of the Internet in the case of cyberattacks and other aggressive actions from abroad. The foreword to the Draft of the RuNet Law 2019 names the United States as Russia's main cyber threat and notes that Russia must take measures to secure the long-term and stable functioning of the Russian segment and improve the reliability of Russia's Internet resources (PZF 608767-7, 2018).

The idea of the RuNet Law (FZ-90, 2019) is to respond to cyber threats by isolating the Russian segment of the Internet from the global Internet and minimizing the amount of Internet traffic crossing Russian borders and transferring through foreign exchange points and servers outside Russian borders. In 2018, half of Russian traffic was transferred through foreign servers. In 2019, the amount is 40% of all traffic of Russian segment and according to implementation

[11] Государственный научно-исследовательский испытательный институт проблем технической защиты информации

plan (APIS, 2017) of the Russian Digital Economy program, the amount will be 10% by 2024.

According to RuNet Law, to support Roskomnadzor Internet operators are obliged to install on their networks "technical equipment to counter threats to stability, security and integrity of functioning of the Russian segment of the Internet." Using this equipment, Roskomnadzor can block prohibited websites and other Internet resources including Telegram Messenger and VPN services. The wording of the RuNet Law is imprecise and the details will probably be in the guidance documents of Roskomnadzor and other state authorities (FZ-90, 2019).

Another imprecise wording of the RuNet Law is the part of the text discussing the creation of Russia's own autonomous domain name system (DNS) no later than the end of 2020. DNS translates URL[12] names into IP[13] addresses and directs the user traffic to the servers. There are 13 DNS root name servers in the global Internet. The root name server contains information about the addresses of the lower level DNS servers, such as the .ru- and .rf domains used in the Russian segment of Internet. For example, when asking for the IP address of www.kremlin.ru, the query goes first to one of those 13 DNS root name servers with the question about the IP address of the DNS server, to whom belongs the IP address in the ru.-domain. Then this server is asked the IP address of the DNS server to whom belongs the IP addresses related to kremlin.ru. Finally, this DNS server will answer with the IP address of www.kremlin.ru.

Technically, it would be complicated, even impossible, to create a new, 14th DNS root name server that was Russia's own. One solution could be that Roskomnadzor's equipment, installed in Internet operators' networks, would also control and coordinate DNS queries, not directing the query to one of the 13 root name servers but by imitating the DNS root name server and directing the query to ru. or rf. server. If the query contains a request for other IP addresses than those belonging to ru. or rf. servers, it could be blocked.

When the RuNet Law is implemented, all the Russian internet traffic crossing Russian borders is transferred through registered Internet exchange points (IX points). Roskomnadzor will establish a traffic-exchange registry. Service providers and companies would be forbidden from using Internet exchange points that are not on the registry. The exchange points would be banned from connecting to companies that do not comply with regulations and rules on the use of the Internet. The traffic between Russian internet segment and the global Internet can be monitored and the connection can be cut at these IX- points (FZ-90, 2019).

By the end of 2019, Roskomnadzor will establish the Center for Monitoring and Managing a Public Communication Network (APIS, 2017). The tasks of the centre include the monitoring of Internet traffic and Public Communication Network (PCN); collecting information on IP addresses and autonomous system

[12] A uniform resource locator (URL) is a reference to a web resource that specifies its location on a network and a mechanism for retrieving it (RFC 1738, 1994).

[13] An Internet Protocol (IP) address is a numerical label assigned to each device connected to a network using the Internet protocol for communication (RFC 760, 1980).

(AS)[14] numbers and communication between them, and traffic routing; and updating information on the topology of the PCN, operating the Internet exchange registry, and adjusting the country's traffic routing. The centre will also manage equipment used to ensure the security of the Russian segment of Internet and the filtering system for Internet traffic used by children. The number of employees in the centre will be 70 (PP-528, 2019). The centre will probably reach initial operational capability (IOC) in 2021–2022 and full operational capability (FOC) in 2024–2025 (PP-528, 2019). The system's efficiency will be checked and improved through regular exercises, participation in which would be mandatory (PZF 608767-7, 2018).

4.3.5 Data Retention Policy

A data retention policy means a state or organizational policy for storing collected for operational use information and ensuring that this information is stored, processed and deleted according to legislation and other regulations. The aim of data retention is to keep important information for future or for reference use and, to organize information so it can be easily searched, accessed and then deleted when it is no longer needed (Rouse, 2014).

The main idea of Russian data retention policy is to store and to process Russian data in information systems locating in the territory of the Russian Federation. The purpose of storing and processing the data in Russian territory is to protect the data against foreign cyberspace exploitation (intelligence) but also to keep the information accessible for Russian security authorities.

In Russia, authorities started to pay attention to digital data retention in the beginning of 2010s. The Data Retention Law (FZ-242, 2014) requires the operators to process and to store personal data of Russian citizens in servers physically located in Russia. Operators had to provide access to this data to Russian authorities. The law applies to foreign companies as well if they are processing or storing the personal data of Russian citizens. Those operators that do not comply with the requirements can be subsequently blocked.

In July 2016, President Putin signed two laws of counterterrorism measures, called the Yarovaya Acts. The laws pose new obligations to the companies that enable the use of instant messaging, social networks, operators of multiplayer games and various websites enabling user-generated content or messages and other companies supporting online communications. Telecom operators are obliged to store, in servers in Russian territory, the content of all telephone calls and SMSs for six months and their metadata for three years, supply them with the personal data of users, and provide that information to law enforcement authorities if needed. Organizers of information distribution on the Internet must provide decryption keys to the FSB (FZ-374; FZ-375, 2016). These measures are

[14] An autonomous system is a set of routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within the AS, and using an exterior gateway protocol to route packets to other autonomous systems (RFC 1930, 1996).

part of the data retention policy, but they also support surveillance of the Russian segment of the Internet.

4.3.6 Surveillance of the Russian Segment of the Internet

The surveillance and monitoring of the Russian Internet traffic are part of the struggle of Russian authorities against internal cyber threats. In Soviet Union, the security services had a strong influence to Soviet society and people's life. The Committee for State Security of Soviet Union, the KGB was responsible for internal security and foreign intelligence since 1954 including signal intelligence (SIGINT). After the Soviet coup d'état attempt in August 1991, the KGB was divided into three parts – foreign intelligence, security service and SIGINT. The Foreign Intelligence Service (SVR) took over the foreign intelligence activities of the KGB (Global Security, 2014a). The internal security functions of the KGB were assigned to the Federal Counterintelligence Service (FSK), which in 1995 was reorganized into the Federal Security Service (FSB) (Global Security 2014b).

The KGB's 8th Directorate (government communications) and 16th Directorate (Signal Intelligence) were combined into the Federal Agency for the Government Communications and Information, FAPSI in 1991. In 2003, FAPSI was reorganized into the Special Communications and Information Service. (N&O Column, 2009.) In the same year, the FSB took over Special Communications and Information Service. Primary functions and tasks of the FSB include law enforcement, counterintelligence, domestic surveillance, and internal intelligence functions including internet surveillance and operative-investigation activity. According to the Russian Federation legislation, operative investigation activity10 is the following:

> activity carried out publicly and privately operational units of state bodies authorized by the present Federal Law, within their powers by conducting search operations in order to protect life, health, rights and freedoms of man and citizen, property, security, society and the state from criminal encroachments. (FZ-144, 1995; PMS-6, 2008)

In carrying out operative investigation activity, the security organizations of the Russian Federation can control postal, telegraph and other communications, listen to telephone conversations, collect information from technical communication channels and acquire computer information. In the operations, they can use information systems and other technical and other means, without prejudice to the life and health of people and do not harm the environment. The legal grounds for carrying out operative investigation in addition to criminal cases are, for example, the following (ZF-144, 1995; PMS-6, 2008):

- information about signs of a wrongful act being prepared, or committed, even if there is insufficient data to resolve the question of a criminal case
- events or actions, endangering the state, military, economic, environmental or information security of the Russian Federation.

The tool for FSB Internet surveillance is a system called SORM[15], the system of the technical means to enable the functions of operative-investigation activity. The operational capabilities of SORM systems have been improved from the 1990s SORM 1 to SORM 3. SORM 1 collected mobile and fixed line telephone calls. SORM 2 also collects Internet traffic (Slugin, 2012; Soldatov & Borogan, 2015). SORM 3 collects all kinds of communication from social networks, Wi-Fi, e-mails, Internet traffic, mobile calls, and voice-over-Internet protocol (Soldatov & Borogan, 2015).

Telecom operators and Internet service provider shad to apply for a license for the commercial and other activities from Roskomnadzor, which approves the applications in cooperation with the FSB. The applicant signs an agreement with the FSB on cooperation in internet monitoring (TAdviser, 2016). Internet service providers (ISP) are required to provide the FSB with statistics on Internet traffic that passes through their servers. ISPs are also required to install SORM devices on their servers, routing the traffic in real time through the FSB's local offices (PP-538, 2005). If the operator is small, instead of installing a SORM system and providing a connection to the local FSB post, FSB can ask the operator to run tcpdump on the traffic of interest (TAdviser, 2016).

In April 1995, President Boris Yeltsin signed a decree on data encryption in Russia (UP-334, 1995) which restricts the use of encryption software to only those programs approved by FAPSI. For a company in Russia to use encryption it must be preregistered with FAPSI. To register with FAPSI, users are required to assess the degree of confidentiality needed. The decree provided no indication as to what methods of encryption (if any) are authorized by FAPSI, and users must consult the encryption providers who can only discuss encryption upon gaining clearance from the FAPSI registration authorities. The decree also instructed the Russian Federation Customs Committee to ban the import of any encryption facilities which lack a FAPSI-approved license (UP-334, 1995).

4.3.7 Censorship in the RuNet and the Ban on Anonymity

After the demonstration in December 2011 against the Russian parliamentary election results, Russian leadership realized that the Internet can be used to spread information and bypass the official information channels and agitate people to participate in demonstrations. For this reason, they introduced legislation for censorship of the Russian segment of the Internet and to ban user anonymity online. Even though censorship and the banning of user anonymity are mainly not information-technological (i.e. cyber) but information-psychological issues, they are discussed in this section.

The legislation process to block unwanted websites started in 2012. The "Black list" Law (FZ-139, 2012) protects children from harmful information on drugs and suicides as well as from child pornography. According to the Black List Law, Roskomnadzor informs the website's owner about forbidden content.

[15] Система технических средств для обеспечения функций оперативно-розыскных мероприятий

If the content is not removed within three days, Roskomnadzor requires Russian telecommunication operators to block any access to this site (FZ-139, 2012).

In 2013, two laws were passed mandating Roskomnadzor to block websites containing harmful or extremist material. Amendments to the Federal Law on the Protection of Children (FZ-135, 2013) defines information on participation in unsanctioned protests or riots harmful to the health and development of children. Roskomnadzor can block access to these harmful pages. Amendments to the Federal Law on Information, Information Technology and Protection of Information (FZ-398, 2013) allows Roskomnadzor, at the request of the prosecutor-general's office (PGO), to block access to information classified by the PGO as extremist or threatening to public order without a court order.

In late autumn 2017 (FZ-327, 2017), Roskomnadzor was mandated to block access, without court order, to information which is produced by proscribed organizations and which promotes protests or mass riots or provides access to such information. In April 2018, Roskomnadzor was mandated to block access, according to court order, to information and content defaming a public figure or company if the information is not removed (FZ-102, 2018).

In 2014, Russian authorities started to develop legislation to ban anonymity in the Russian segment of the Internet and improve identification of Russian internet users. Amendments on Federal Law on Information, Information Technologies and Protection of Information, herein after the Blogger Law (FZ-97, 2014), requires a blogger, with a site with more than 3,000 daily visitors, to officially register with Roskomnadzor. The Blogger Law defines a person who is able to receive, transmit, deliver or process the electronic messages of Internet users as an organizer of distribution of information (ODI). An ODI is obliged to retain and store Russian user data for six months and disclose that information to law enforcement authorities. A governmental decree (PP-758, 2014) issued in July 2014 obligates Internet users, when connecting to Wi-Fi, to supply his telephone number, and Internet providers to retain and make this data available to the authorities for six months.

In July 2017, two laws were signed improving identification of users and banning user anonymity in communication networks. Providers of messaging applications (FZ-241, 2017) were obliged to ascertain the identity of users and telephone numbers. Telecom operators were required (FZ-245, 2017) to activate only SIM cards registered with user identification. The Amendment to the Law on Information (FZ-276, 2017) prohibits virtual private network (VPN) services and Internet anonymizers in Russia. The law (FZ-276, 2017) gives Roskomnadzor authorization to block sites that are forbidden or which provide instructions on how to circumvent government blocking, allows Roskomnadzor to cooperate with the FSB to identify users of anonymizers and block them.

4.3.8 Special-purpose Telecommunication Networks

The unified telecommunication network of the Russian Federation consists of telecommunication networks of the following categories located in the territory of the Russian Federation:

- public communication network
- dedicated communication networks
- technological communication networks connected to the public communication network
- special-purpose communication networks
- other communication networks

The public communication network is intended for the provision of telecommunication services to any user of telecommunications services in the Russian Federation. The public communication network has access to public communication networks of foreign countries. In the future, when the RuNet Law is enacted, this connection to abroad will be operated through registered IX points where authorities can monitor the traffic. Dedicated telecommunication networks[16] are providing telecommunications services to a limited number of users or groups of users. Dedicated networks can interact with each other.

Dedicated communication networks do not have access to the public communication network, nor to the public communication networks of foreign countries. Technological communication networks are designed to ensure the production activities of organizations and the management of technological processes in production. Technological communication networks can be connected to technological communication networks of foreign organizations only to ensure a single technological cycle.

Special purpose communication networks are intended for the needs of state authorities, the needs of national defense, state security and law enforcement. Service of Special Communications and the Information Service of the Federal Security Service (FSO) of the Russian Federation ensures the operation, maintenance and development of the t Russian State Network, RsNet (PFSO-487, 2009). One of the special-purpose communication networks is the Single Network of Data Transmission (SNDT) for state agencies of RsNet, which is used by federation- and subject-level state organizations, such as the following (PFSO-443, 2016):

- Administration of the President of the Russian Federation
- Office of the Council of the Federation of the Federal Assembly
- Office of the State Duma
- Office of the Government of the Russian Federation
- the offices of the Constitutional Court
- the Supreme Court
- the Supreme Arbitration Court
- General Prosecutor's Office
- Investigative Committee at the Prosecutor's Office

Another special purpose communication network is Russian Armed Forces' own closed intranet. This intranet is called the Closed Data Transmission Segment

[16] Выделенная сеть связи

(CDTS)[17] and it is not connected to the global Internet. CDTS is constructed on the leased infrastructure of Rostelecom, Russia's biggest telecom operator. The computers of CDTS are protected against, for example, connections by uncertified USB drives and external hard drives. The system has its own e-mail service, which allows the transfer of sensitive information, including secret and top secret documents (Rjabov, 2019).

The Armed Forces of the Russian Federation have begun to create a closed digital communication system called the multi-service transport communications network (MTSS). The first phase of work will be completed by the end of 2019, and the project will be fully implemented in two years. MTCC will not have traffic exchange points connecting it with the Internet. MTSS will be based on its fiber-optic networks divided into zonal trunk channels. The archive will be located on the servers of the Ministry of Defense and will be constantly duplicated in order to preserve data in case of damage to one of them. This means the army will receive its own private cloud storage. In addition, MTSS will have its own search engine (Ramm, Kozatsenko & Stepovoi, 2019).

4.3.9 Effort to Replace Imported ICT with Russian-produced ICT

For Russia, one of the most difficult questions to respond to cyber threats is that the country is lagging behind the leading foreign countries in the development of competitive information technology, including supercomputers. This gap strengthens the Russian perception of its strategic vulnerability in cyberspace. For almost twenty years, Russia has tried, without success, to replace imported ICT software with Russian-made counterparts, and it seems that they will not succeed in the near future either. Russia is attempting to compensate for this lack mainly by isolating the Russian segment of the Internet and by protecting the CIIRF.

One of the ways to correct Russia's technical backwardness in ICT and protect it against cyber threats is to develop the country's own IT sector by improving its research, development, and production of information technology (UP-646, 2016). To improve the security of its information infrastructure, Russia has to replace imported ICT software and equipment with Russian-made counterparts and lay the foundation for technological independence in ICT production (UP-203, 2017). President Putin (2018) stated that Russia needs to build its own digital platforms, ones that should be compatible with the global information space. The ISD 2000 (PP-1895, 2000) had already identified the backwardness of Russian ICT as one of the main threats to the country's information security.

In January 2016, following the results of the Internet Economy Forum, President Putin ordered the establishment of the Competence Center for Import Substitution in Information and Communication Technologies (CICT). CICT is an autonomous non-profit organization, the task of which is to solve practical, methodological and organizational issues related to the implementation of state policy on import substitution. The tasks of the CICT are support of state bodies and

[17] Закрытый сегмент передачи данны (ЗСДП)

organizations on the issues of import substitution of software and ICT equipment, and the identification of barriers and factors that impede import substitution in the field of ICT and the preparation of proposals for their elimination (CICT, 2019). The aim of activities of CICT is to ensure technological independence and security of hardware and data processing infrastructure. CICT is planned to have full operational capability no later than in March 2020. The aim is that by no later than the end of 2024 all the objects of information infrastructure of the Russian Federation, including data processing, will use Russian-made computers, servers and communication equipment (APIS, 2017).

5 INTERPRETATION OF RUSSIAN CYBER THREAT PERCEPTION

5.1 Theory of Strategic Culture

The concept of political culture, defined as a subset of the beliefs and values of a society related to the political system, was developed in the 1960s (Almond & Verba, 1963). In 1977, as a researcher from RAND[18], Jack L. Snyder implemented the ideas of political culture in security studies in his study The Soviet Strategic Culture. He stated that it is possible to understand and to explain Soviet strategic thinking and state behaviour, which he called strategic culture, by identifying historical, institutional, and political factors influencing on Soviet leadership´s strategic thinking (Snyder, 1977). After Snyder, the theory of strategic culture developed through three generations of scholars, each with their own conceptual and methodological approach (Johnston, 1995a). The theory of strategic culture, including its evolution, insights and shortcomings, is discussed in article IV, "Strategic Culture Theory as a Tool for Explaining Russian Cyber Threat Perception" (Kari, 2019) and in article VI, "Theory of Strategic Culture: an Analytical Framework for Russian Cyber Threat Perception" (Kari & Pynnöniemi, 2019).

In his book Cultural Realism: Strategic Culture and Grand Strategy in Chinese History (1995b), Alastair Iain Johnston, one of the most important representatives of the third generation of strategic culture research, studied the character and linkages of Chinese strategic culture to the use of military force against external threats. In his methodological framework, cultural orientations were the independent variable and military strategy was the dependent variable. Johnston's definition for strategic culture is the following:

[18] American nonprofit global policy think tank, offers research and analysis to the US Air Forces

> An integrated system of symbols (e.g. argumentation, structures, languages, analogies, metaphors), which acts to establish pervasive and long-lasting grand strategic preferences by formulating concepts of the role and efficacy of military force in interstate political affairs, and by clothing these conceptions with such an aura of factuality that the strategic preferences seem uniquely realistic and efficacious. (Johnston, 1995b)

Strategic culture (Johnston, 1995b) is a set of persistent and consistent historical patterns of how state leadership thinks about the use of force to achieve political goals. The preferences originate in the historical experiences related to the threat and use of force by the state and are influenced by the philosophical, political, cultural, and cognitive experiences and characteristics of the state. (Johnston, 1995b)

According to Johnston, strategic culture consists of a central paradigm and a set of strategic preferences. The central paradigm describes the nature of the conflict and the perception of the enemy and threat as well as how to respond to that threat. Strategic preferences are assumptions about what options are the most effective against a particular threat (Johnston 1995a). Different states have their own strategic culture, developed over a long period. Factors influencing strategic culture might be historical, technological, political or organizational. Knowing these factors might make it possible to explain how and why a state experiences a threat in a certain way. Understanding the strategic culture of another country is vital because it helps to understand its strategic policy variables and the underlying threat assessments and situational awareness in specific situations (Booth, 2005). This supports drawing of estimations and predictions on state behaviour in specific situations in the future.

Strategic choices are based more on historically rooted strategic preferences than, for example, on changes in the strategic environment (Johnston, 1995b). Strategic culture can change, but it changes slowly. Factors, which can change strategic culture are external shock, disharmony and a clash of the core principles of strategic thinking, and the state leadership can change strategic culture by adopting a new approach to foreign policy questions. (Lantis, 2006.) External shock can change nation´s historical narratives and construct new alternative norms. An example of the influence external shock to strategic culture, is the change of German politics because of the humanitarian catastrophe in Bosnia in the 1990s. The essence of German strategic culture after the World War II, pacifism, hindering use of military forces outside Germany, was replaced by the sending troops to Bosnia for IFOR- operation.

An example of disharmony and a clash of core principles of strategic thinking is Japan, which had refrained from use of military force until it sent military personnel to the United Nations peacekeeping operation in East Timor for protect democracy. Third factor changing strategic culture is the role of state leadership. Leaders can follow the direction of strategic culture or they can change strategic culture by adopting a new approach to foreign policy questions. The countermeasures taken by the USA after the 9/11 attack is an example of change of strategic culture caused by these three factors. The external shock made the leader, President Bush, declare war on terrorism, which was a shift to a new kind of policy in a new kind of threat environment. New policy changed the centre of gravity to homeland defense and gave rise to a new doctrine of pre-emption with the use of military forces, which can be considered disharmony and a clash of the core principles of strategic thinking (Lantis, 2006).

This thesis argues that the theory of strategic culture is a suitable theory for exploring and explaining the Russian vision of cyber conflicts, its enemies, cyber threats and preferences for responding to cyber threats. Russian cyber threat perception is not a separate part of Russian general threat picture and it can be explained and examined by using the theory of strategic culture. Theory of strategic culture is used in this thesis to interpret and to explain the results of data analysis presented in Chapter 4. In this thesis is applied Johnston's definition of strategic culture and his methodological framework. Even though Johnston's analytical framework is almost 25 years old, it was selected as the theory for this thesis because Johnston's approach is still valid. The division of strategic culture into a central paradigm and strategic preferences provides a sufficient framework to explain the Russian cyber threat perception and the country's response to cyber threats. The central paradigm of Russian strategic culture corresponds to the Russian threat perception and strategic preferences correspond to Russia's response to such threats. The factors influencing Russian strategic culture are independent variables. The central paradigm and strategic preferences of Russian strategic culture are then viewed as dependent variables.

This chapter answers research question "How does Russian strategic culture explain Russia's cyber threat perception and its response to that threat?". First, the factors and elements of Russian strategic culture are described. After that, Russian cyber threat perception and Russia's response to that threat is explained and interpreted in the light of Russian strategic culture.

5.2 Russian Strategic Culture

Factors influencing strategic culture can be historical, geographical, and political or they can relate to organization or technology. According to Johnston (1995b), historical factors have a predominant influence on the formulation and outcome of a state's strategic culture. These historical factors are influenced by the political, cultural and cognitive characteristics of the state. Technology, threat level and organizational structures are of secondary importance. This thesis composes the factors that influence Russia's strategic culture into four groups: history, geography, technology, and the political system and worldview of Russian leadership. In addition, this thesis discusses the changed rules of war as disharmony and a clash of the core principles of strategic thinking that have an influence on Russian strategic culture.

One of the basic assumptions of Russian strategic culture is that the international arena is a dangerous, chaotic, and volatile battlefield (Sinovets, 2016). The National Security Strategy of the Russian Federation (UP-683, 2015) states that the use of force in international politics is increasing. Long periods of Russian history have been dangerous, chaotic and related to the use of force to fight enemies, but also to expand the area and create buffer zones and easily defensive borders. Russia has been attacked many times. Mongols destroyed Kiev in 1240 and ruled Russia until 1380. After that, Russia has been attacked by Sweden in 1700 and by Napoleon in 1812. Germany attacked Russia in both World Wars. The German attack in the Second World War caused enormous casualties to the Soviet Union (Kirkinen, 2000). These historical experiences (Facon, 2017; Eitelhuber, 2009) have created a sense of vulnerability and fear of invasion in Russian strategic culture, the so-called Barbarossa syndrome[19] (Cimbala, 2013).

Russian leadership has reinforced this perception of threat by using the narrative of Russia as a besieged fortress. According to President Putin, the Soviet Union was a besieged fortress constantly under threat of attack by the West (Aron, 2008). NATO enlargement and war in eastern Ukraine have bolstered this narrative and brought back the Soviet-era perception of permanent war between Russia and the USA. The Military Doctrine 2016 names NATO as one of the main external military dangers. The danger consists of NATO's overall capacity, the organization's potential violations of international law, and the encroachment of its military infrastructure on Russia's borders (MDRF, 2014). The Clausewitzian belief in the use of force has been one of the fundamental elements of Russian strategic culture. The military has had a main role in the protection of Russia and the Soviet Union.

Russian history is also full of internal disturbances starting from the time of troubles (1606–1613) to the revolutions in 1917 and to the breakup of the Soviet Union at the beginning of 1990s, which was a traumatic historical incident for the Russian people (Ermarth, 2006; Eitelhuber, 2009). During Putin's regime, the role of the security services, the Chekists, has also grown because of increased fear of internal disturbances (Facon, 2016). The exaggeration of internal threat (Felgenhauer, 2005) have been caused by the KGB culture of the Russian leadership (Facon, 2016) and the threat perception centered on the so-called colour revolutions (Skak, 2016) have reinforced the fear of internal enemies and increased the perception of vulnerability. It is the Russian view that the Arab Spring was sponsored by Western intelligence services, which also attempt to influence Russian internal affairs by sponsoring political opposition.

Geography has an influence on Russian strategic culture. The lack of natural borders has created a sense of vulnerability and a need for a buffer zone, political and military control of neighbouring spaces, and territorial expansion to natural, easily defensible borders (Ermarth, 2006; Facon, 2016). Russia's technological inferiority and its backwardness in the development of high technology have also had an influence on the country's strategic culture. The factors influencing Russian strategic culture and the central paradigm of Russian strategic culture is described in Figure 14.

[19] Operation Barbarossa was the code name of the German invasion of the Soviet Union in June 1941, which completely surprised Soviet Armed Forces and Soviet leadership

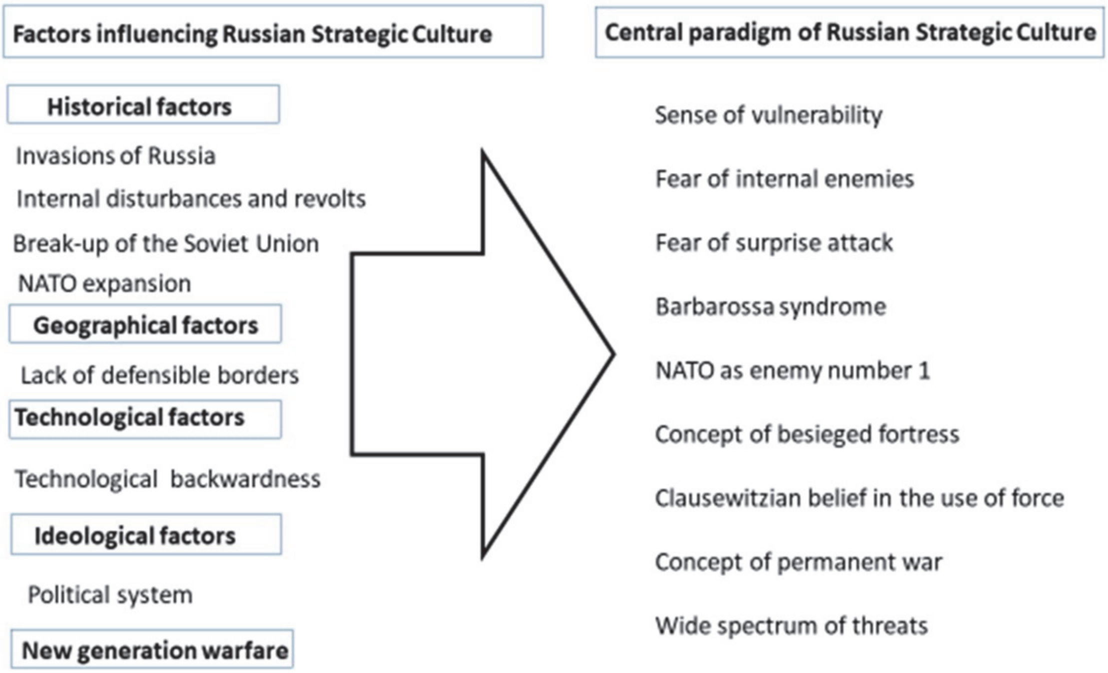


FIGURE 14 Factors and Central Paradigm of Russian Strategic Culture

Even though the central paradigm of Russian strategic culture has remained unchanged for centuries, disharmony and the clash of the core principles of strategic thinking have influenced the role of conflict, the country's threat perception, and its strategic preferences in the 2010s.

The collapse of the Soviet Union in 1991 is an example of a shock that has influenced Russian strategic culture. The militarily strong, sometimes aggressive besieged by Western states fortress of Soviet Union collapsed and was replaced by liberal Russia with democratic aspirations as well as economic and political cooperation with the West. In 1996 the Kremlin changed Russian strategic culture by adopting a new approach to foreign policy. Yevgeni Primakov, a patriotic pragmatist, replaced the Western-oriented foreign minister Andrei Kozyrev in January 1996 and the focus of Russian foreign policy shifted from the West to Eurasia. Primakov, who used to serve before the post of foreign minister as the head of Federal Intelligence Service, focused on ensuring Russia's status as a global power (Lynch, 2002).

In the so-called Primakov Doctrine, Primakov opposed the global domination of the USA and supported a multipolar system, with Russia as one of the poles. He tried to dilute the international power of the USA, supported a strategic partnership between China and Russia as well as union with Belarus, and wanted to have the Caucasus and Central Asia under the sphere of Russian influence. The war in Kosovo and the NATO bombing of Serbia were the final disharmony of the post-Soviet democratic West-oriented core principles and when the so-called siloviki[20] seized power in the Kremlin in 2000 Russian strategic culture started to resemble the strategic culture of Soviet Union.

The Chief of the General Staff of the Armed Forces of Russia, General Valery Gerasimov (2013), gave a speech in 2013, in which he stated that the rules of war have changed. The Clausewitzian belief in the use of force to achieve political aims can still be seen, but the role of non-military means to achieve political and strategic goals has grown. In many cases, non-military means have exceeded the power of weapons in their effectiveness. The lines between war and peace have been blurred. The concept of the permanent war zone is also introduced in the Military Doctrine 2014. Asymmetrical actions, such as the use of special forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as information operations are also part of the changed rules.

5.3 Elements of Russian Strategic Culture in Cyberspace

Russian cyber threat perception and response to cyber threat can be explained by the factors and elements of Russian strategic culture. Factors, influencing to Russian strategic culture, as sense of vulnerability, fear of surprise attack and invasion, narrative of Russia as besieged fortress and concept of permanent war, influence to Russian strategic culture also in cyberspace. The elements of Russian strategic culture in cyberspace are the central paradigm, meaning the Russian cyber threat perception, and strategic preferences describing Russia's response to cyber threats. The central paradigm includes assumptions about the nature and role of cyber conflict and the subjects and the objects of cyber threat. The interconnection of the model of the Russian cyber threat perception with factors and elements of Russian strategic culture is described in Figure 15.

[20] a politician who came into politics from the security or military or similar services

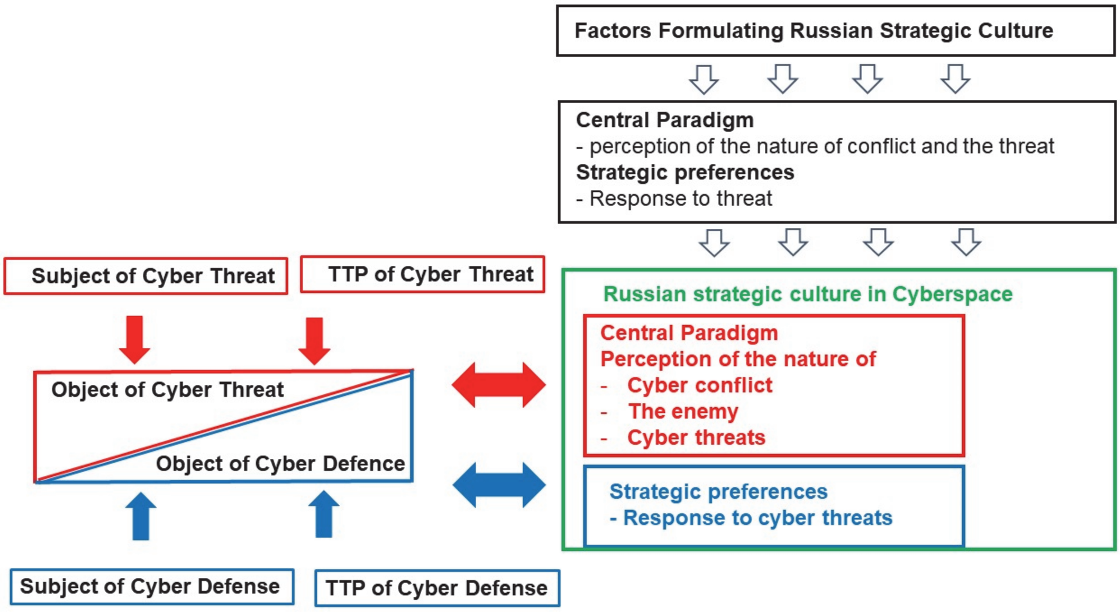


FIGURE 15 Interconnection of the model of Russian cyber threat perception with factors and elements of Russian strategic culture

According to the Russian views, the number and severity of threats to Russia have increased in cyberspace, and those threats are shifting to Russia's internal sphere (PP-2796, 2014). Russia's national interests can be threatened in or through cyberspace also internally. Terrorists and extremists may direct cyberspace attacks to strategic targets to disrupt the management and decision-making system and to paralyze Russia's strategic leadership. In addition, cybercriminals may threaten Russia´s national interests in or through cyberspace by penetrating the state information systems (see SBRF, 2012; RBA, 2013; SBRF, 2013; MDRF, 2014).

For Russia, the most difficult question in responding to cyber threats is that the country is lagging behind the leading foreign countries in the development of competitive information technology, including supercomputers, and this gap strengthens the Russian perception of its strategic vulnerability in cyberspace. For almost twenty years, Russia has tried, without success, to replace imported ICT software with Russian-made counterparts, and it seems that they will not succeed in the near future either.

Russia's most important strategic preferences against cyber threats are improved protection of the critical information infrastructure, preparations to isolate the Russian segment of the Internet from the global Internet, intensified surveillance and the ban of user anonymity on RuNet, and the aspiration to replace imported information and communication technology with Russian-produced ICT. Figure 16 describes the central paradigm and preferences of Russian strategic culture in cyberspace.

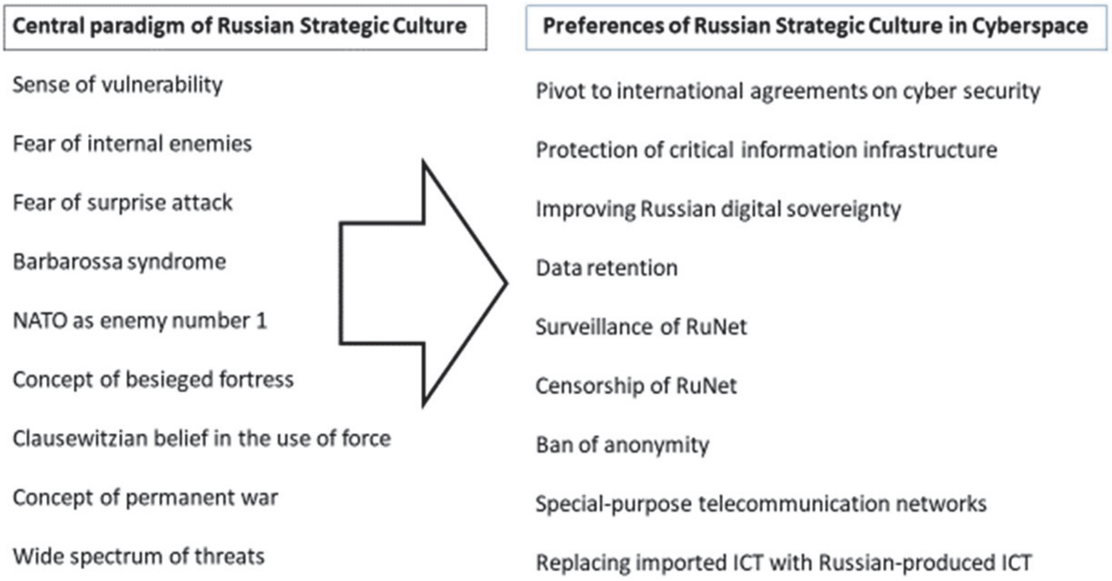

Central paradigm of Russian Strategic Culture
Sense of vulnerability
Fear of internal enemies
Fear of surprise attack
Barbarossa syndrome
NATO as enemy number 1
Concept of besieged fortress
Clausewitzian belief in the use of force
Concept of permanent war
Wide spectrum of threats
Preferences of Russian Strategic Culture in Cyberspace
Pivot to international agreements on cyber security
Protection of critical information infrastructure
Improving Russian digital sovereignty
Data retention
Surveillance of RuNet
Censorship of RuNet
Ban of anonymity
Special-purpose telecommunication networks
Replacing imported ICT with Russian-produced ICT

FIGURE 16 Central paradigm of Russian strategic culture and strategic preferences in cyberspace

One of the basic assumptions of Russian strategic culture, in terms of Russia's strategic preferences for isolating the Russian segment of Internet and improved protection of the CIIRF, is that the confrontation between Russia and the USA has escalated and expanded into cyberspace. An assumption, based on the Clausewitzian belief in the use of force, is that the Western countries are surrounding Russia and waging permanent war in cyberspace as well. The battle to disrupt Russia's digital sovereignty is waged every day (Sinovets, 2016). One of Russia's national interests is to maintain the stability, safety and independence of the Russian segment of the Internet (UP-646, 2016). Because the war is waged inside Russia as well as in the information space, where a traditional military force is of little use, the role of the Federal Security Service of the Russian Federation (FSB) has increased.

Historical, cultural and geopolitical experiences and ideology have built up the threat perception based on a sense of vulnerability. The Western powers try to maintain their positions in the world by containing "alternative centres of power," namely, Russia (UP-640, 2016). The sense of vulnerability has created a concept of Russia as a besieged fortress. Russia views itself as a besieged fortress also in cyberspace. ICT is used for military-political purposes against the sovereignty and territorial integrity of Russia. This besieged fortress narrative can also be seen in Russia's cyber threat perception. Putin (2016) has also stated that because of the risks inherent to digitalization, Russia has had to strengthen its defense against cyber threats targeted, for example, at Russian infrastructure, the country's financial system, and the state's leadership and management. The number and severity of dangers and threats have increased in the information space (MDRF, 2014). Certain states are attacking and collecting intelligence on the Russian information infrastructure for military and political purposes (UP-646, 2016).

The USA has been named as the main subject of the external cyber threat. According to Russian view, the USA uses its technological superiority to dominate the information space (UP-646, 2016).The USA is trying, according to President Putin (2015), to destroy strategic balance, change the balance of power, and dominate and dictate their will to anyone. This has caused the Kremlin to feel a sense of vulnerability in cyberspace. The Clausewitzian belief held by Russian leadership on the use of force as a part of politics can be seen in the statements regarding preparations for information warfare and how the aspirations of Western countries to change cyberspace into a war zone threaten Russia's strategic interests in cyberspace (UP-646, 2016) and could lead to a virtual arms race (YA, 2009; RBA, 2013; SBRF, 2013).

The Kremlin's concern over internal enemies has grown after the Arab Spring, when uprisings in some Arab countries forced a change in leadership. This fear of internal enemies can be seen in Russia's cyber threat perception. The exaggeration of the internal threat (Felgenhauer, 2005) caused by the KGB culture of Russian leadership (Facon, 2016) and the threat perception centered on the so-called color revolutions (Skak, 2016) have increased this perception of vulnerability. It is the Russian view that the Arab Spring was sponsored by Western intelligence services, which also attempt to influence Russian internal affairs by sponsoring political opposition (UP-646, 2016).

6 OVERVIEW OF THE ARTICLES

This chapter presents the objectives and finding of the articles and their relation to this thesis. The author of this thesis wrote Articles II, III, IV and V. Article I, “Russia: A Cyber Fortress Besieged,” was written with Adjunct Professor Rauno Kuusisto. Kari was the main contributor to Article I, and Kuusisto’s role was to support and guide Kari in the process of writing his first conference paper.

Article VI, “Theory of Strategic Culture: an Analytical Framework for Russian Cyber Threat Perception,” was co-written with Assistant Professor of Russian Security Policy Katri Pynnöniemi from the National Defense University and Helsinki University.

6.1 Article I: Russia: A Cyber Fortress Besieged

Kari, M and Kuusisto, R (2017). Russia: A Cyber Fortress Besieged. The 16th European Conference on Cyber Warfare and Security. Dublin, Ireland. 29–30 June 2017. (ISBN 978-1-911218-43-2, E- Book ISBN 978-1-911218-44-9). pp. 593–601.

Research objectives

Article I answers research question: “What is Russia’s cyber threat perception?” The paper examines and describes the Russian perception of the cyber threat to Russia based on official documents. The aim of this paper is to build a description of the Russian perception of cyber threats and the targets of cyber threat publicly described by the Russians. Grounded theory was used as the research method, an appropriate approach because little theoretical and structured information has, to date, been published on the Russian response to cyber threats. The data are drawn from official Russian documents such as strategies, doctrines, laws, and presidential decrees. The keywords of the Article I are Russia, cyber threat, cyberspace, cyber operation, critical information infrastructure and information resources.

Findings

The findings of Article I indicate that the Russian cyber threat assessment reflects the tension in the international situation. One of the axioms of Russian history is that the Soviet Union has been a besieged fortress, surrounded by potential enemies and under constant threat of attack from the West. After the annexation of Crimea and the wars in eastern Ukraine and Syria, the Kremlin's image of Russia is once again that of the besieged fortress, surrounded by enemies and under threat of attack. This perception has extended to cyberspace. The Russian cyber threat assessment is based on the besieged fortress narrative. The subjects of the cyber threat are Western intelligence and special services along with terrorists and extremist movements. The branches of Russian administration along with ministries and agencies emphasize different issues in their cyber threat assessments, but the basic structure of the targets and threats is common.

The information security doctrine from 2000 names the underdevelopment and backwardness of Russian information technology as a threat to the country's information security. Over the past decade, Russia has not managed to reduce the lead of Western countries in this area. The insufficient level of development of domestic information technology, services and production capabilities and a lack of supercomputers generate dependence on foreign information technology.

Cyber-attacks and cyber espionage against Russia have intensified, which requires better management of information security by Russian authorities. The main opportunities to improve information security are increasing the monitoring of RuNet, creating international legal norms to prevent uses of the Internet that are harmful to Russia, and the development of Russia's own information technology industry, including research and development activity.

Summary and the relation to the whole

Article I analyses Russian cyber threat perception. This perception is based on the besieged fortress narrative, which also dominates the general Russian threat perception. Article I was written before some of the most important cyber security documents, such as the Law on Security of Critical Information Infrastructure of the Russian Federation (FZ-187, 2017) and its follow-up laws, directives and other documents were published. Therefore, it can be considered a general introduction for the more detailed research on the protection of critical information infrastructure of the Russian Federation, and Russian cyber threat perception and Russia's response to that threat presented in the following articles.

6.2 Article II: The Concept of the Critical Information Infrastructure of the Russian Federation

Kari, M (2018). The Concept of the Critical Information Infrastructure of the Russian Federation. The 13th International Conference on Cyber Warfare and Security. Washington DC, USA. 8–9 March 2018. (ISBN 978-1-911218-74-6, E-Book ISBN 978-1-911218-73-9) pp. 543–551.

Research objectives

Article II answers research question "What are the most important objects to protect in Russia's cyber threat perception?" In Article II, the aim is to understand and examine the concept of the critical information infrastructure of the Russian Federation (CIIRF) as one of the most important subjects to protect against cyber threats. The Article outlines the development of the Russian concept of the CIIRF over the last two decades. The concept of CIIRF helps to understand Russian threat perceptions in cyberspace, and it serves as one of the basic terms in the research on Russian information security management. The paper briefly describes the Russian definition of two terms: information infrastructure and critical infrastructure. After that, is examined the evaluation of the Russian term CIIRF using definitions found in Russian official documentation since the publication of the Information Security Doctrine in 2000. The keywords of this paper are Russian Federation, critical information infrastructure and critically important object.

Findings

One of the findings of the paper is that the concept of the CIIRF has been developing in Russia since 2000. Information Security Doctrine (ISD 2000) was the first official document to discuss the idea of the CIIRF. A list of the most important objects for ensuring the information security of the Russian Federation were drafted at the end of the 1990s, when the international political situation was less tense than it is today. The list in ISD 2000 of these most important objects was broad, fragmented and included many that have not been reiterated in later versions of the CIIRF.

The Bill for Ensuring the Information Security of Critical Important Objects of Information and Telecommunications Infrastructure 2006, hereinafter the CIO Bill 2006, defined the critically important objects (CIO) of the information and telecommunications infrastructure. CIO is an object that, when its functioning is violated, it can lead to an emergency or to significant negative consequences for defense, security, international relations, the economy of the RF, or infrastructure of the country, or for the livelihoods of people living in the territory concerned for a long period. The CIO Bill 2006 included a list of CIOs focused more on security and defense than the list in ISD 2000.

According to the Main Directions of State Policy in the Security of Automatic Control Systems for Production and Technology Processes in Critical Important Infrastructure Objects of the Russian Federation (SBRF, 2012), hereinafter CII Policy Directions 2012, the CIIRF is a complex of automated systems for managing CIOs and for enabling their connections with information networks. These objects are used for state management and for ensuring defense capability as well as security and law and order, and their violation may have severe consequences. The CIIRF is defined in the CII Bill 2013 in the same way as it was defined in the CII Policy Directions 2012.

After two versions of a bill for the security of the CIIRF (2006 and 2013), the State Duma finally passed the third version in July 2017. According to the definition of the CII Security Law 2017, the CIIRF consists of "objects of critical information infrastructure, as well as the telecommunication networks used to organize the interaction of these objects and the objects of the CIIRF are information systems, information and telecommunication networks, and automatic control systems of the subjects of the critical information infrastructure."

The CII Security Law 2017 contain a list of the objects of critical information infrastructure, including the information systems, information and telecommunication networks of state authorities and the most important industrial sectors of and societal activity. The definition of CIIRF and the objects of CIIRF in the CII Security Law 2017 are the results of a long assessment and they can be considered as stable, long-term definitions.

Summary and the relation to the whole

Article II examines the Russian term critical information infrastructure of the Russian Federation, using definitions found in Russian official documentation since the publication of the Information Security Doctrine in 2000. The aim of Article II was to identify the Russian definition for the critical information infrastructure, which is one of the main targets of cyber threats in the Russian cyber perception. This definition was needed to get theoretical background for the protection of CIIRF. In this thesis, Article III discuss the protection of Russia's critical information infrastructure.

6.3 Article III: The Protection of Russia's Critical Information Infrastructure

Kari, M (2018). The Protection of Russia's Critical Information Infrastructure. The 17th European Conference on Cyber Warfare and Security. Oslo, Norway. 28–29 June 2018. (ISBN 978-1-911218-85-2, E-Book ISBN 978-1-911218-86-9) pp. 533–540.

Research objectives

Article III answers research question "How is Russia responding to cyber threats?" Article III discuss the protection of the critical information infrastructure of the

Russian Federation (CIIRF). The concept of the CIIRF has been in development for two decades. Together with this development there has also been constant debate on how the CIIRF should be protected. The aim of Article III is to investigate the roles and responsibilities of Russian state authorities in responding to cyber threats, especially between the Federation Security Service (FSB) and the Federal Service for Technical and Export Control (FSTEC). The keywords of the paper are Russia, critical information infrastructure, cyber threat, FSTEC, FSB and GosSOPKA.

Findings

One of the national interests of the Russian Federation in cyberspace is to ensure stable and uninterrupted functioning of the information infrastructure, primarily of the critical information infrastructure of the Russian Federation (CIIRF) and the integrated telecommunications network of the country in peacetime, in the event of a direct threat of aggression, and in wartime. One of the findings of the paper is that the definition of the CIIRF and the division of responsibilities to protect the CIIRF were confirmed by legislation passed at the end of 2017.

Furthermore, the CII Security Law and related legislation defined the roles of two authorities in the IS management of the CIIRF. The FSB was tasked with creating and operating GosSOPKA (State System of Detection, Prevention and Elimination of Consequences of Computer Attacks to Information Resources of RF), and the FSTEC was named as the federal executive body authorized to ensure the security of the CIIRF.

Summary and the relation to the whole

Article III is a continuation of Article II. Together with Article II, Article III addresses the question of defending the national interests of the Russian Federation in cyberspace. Articles II and III were written by the author of this dissertation alone. The definition of the CIIRF and the division of responsibilities to protect it were confirmed in legislation at the end of 2017. The next phase in the protection of the CIIRF, starting in 2018, is the implementation of these principles.

6.4 Article IV: Strategic Culture Theory as a Tool for Explaining Russian Cyber Threat Perception

Kari, M (2019). Strategic Culture Theory as a Tool for Explaining Russian Cyber Threat Perception. The 14th International Conference on Cyber Warfare and Security. 28 February–1 March 2019, Stellenbosch, South Africa. (ISBN 978-1-912764-11-2, E-Book ISBN 978-1-912764-12-9) pp. 528–535.

Research objectives

Article IV answers research question "How does Russian strategic culture explain Russia's cyber threat perception and its response to that threat?" The increased interest in cyber threats has heightened the need for theoretical tools to study the perceptions of those threats. Article IV argues that strategic culture theory is a suitable tool for exploring and explaining the Russian idea of cyber conflicts, the country's cyber threat perception and its strategic preferences, that is, its options to respond to cyber threats.

The basic assumption of the theory of strategic culture resides in the belief that all nations have their own strategic culture. Strategic culture consists of a central paradigm and a set of strategic preferences. The central paradigm describes the nature of the conflict and the perception of the enemy and threat as well as how to respond to that threat. Strategic preferences are assumptions about what options are the most effective against a particular threat (Johnston, 1995a).

Different states have their own strategic culture, developed over a long period. Factors influencing strategic culture might be historical, technological, political or organizational. Knowing these factors might be possible to explain how and why a state experiences a threat in a certain way. Strategic choices are based more on historically rooted strategic preferences than, for example, on changes in the strategic environment. If the strategic culture does change, it changes slowly (Johnston, 1995b). The keywords of Article IV are strategic culture theory, Russian strategic culture and Russian cyber threat perception.

Findings

The elements of Russian strategic culture can be used as a theory to explain Russian cyber threat perception and the country's response to that threat. The central paradigm of Russian strategic culture, which includes a sense of vulnerability, the besieged fortress narrative, a Clausewitzian belief in the use of force, and a fear of external and internal enemies and uprisings, can also be identified in the Russian cyber threat perception. Russian strategic preferences are reflected in the cyber environment as an increased role for the security services, tightened control of RuNet, improved defense through the creation of buffer zones by RuNet, and the increasing emphasis on digital sovereignty.

Disharmony and the clash of core principles of strategic thinking have influenced the Russian threat perception. The role of nonmilitary means of achieving goals has grown, the role of cyber warfare has increased, and warfare in cyberspace has become permanent.

Russian leadership feels vulnerability in the cyber environment partly for historical and geographical reasons, and partly because of the country's technical backwardness. Russia has been repeatedly attacked throughout its history, a situation that could reoccur in the cyber environment. Much like the country's physical environment, the cyber environment contains no easily defendable borders, especially because most of the ICT is made in the USA and the control of the global Internet is in American hands, which is also the main threat to Russia.

That is one reason why the Kremlin is creating technical possibilities and operational preparedness to isolate RuNet from the global Internet.

The besieged fortress narrative is one reason for the Russian pivot to digital sovereignty and improved protection for the critical information infrastructure of the RF. The fear of internal disturbances has increased the mandate and the responsibilities of security services in the cyber environment. The FSB was tasked to surveil communications in RuNet using the SORM system and to protect the critical information infrastructure of the RF with the GosSOPKA system.

Summary and the relation to the whole

Article IV argues that strategic culture theory is a suitable tool for exploring and explaining the Russian idea of cyber conflicts, the country's cyber threat perception and its strategic preferences, that is, its options to respond to cyber threats. This Article first identifies the specific factors influencing Russian strategic culture then moves on to a discussion of the elements comprising it. These elements, which can also be identified in the cyber environment, include a sense of vulnerability, the narrative of Russia as a besieged fortress, and Russia´s technological inferiority. Methodologically, Article IV is a literature survey based on official Russian documents related to information security. These include the Russian Federation's information security doctrines, draft legislation and laws as well as documents from the RF Security Council and Ministry of Defense. The use of the theory of strategic culture as an analytical framework for Russian cyber threat perception is discussed in more detail in Article VI, which is the theoretical background of the whole thesis. Article IV also updates the cyber threat picture presented in Article I by using information published after January 2017, when Article I was written.

6.5 Article V: Protecting the Besieged Cyber Fortress: Russia's Response to Cyber Threats

Kari, M (2019). Protecting the Besieged Cyber Fortress: Russia's Response to Cyber Threats. The 18th European Conference on Cyber Warfare and Security. 4–5 July 2019, University of Coimbra, Portugal. (ISBN: 978-1-912764-28-0, E-Book ISBN: 978-1-912764-29-7) pp. 685-691.

Research objectives

Article V argues that strategic culture theory is a suitable tool for exploring and explaining the Russian cyber threat perception and options to respond to cyber threats. Article V identifies the specific factors influencing Russian strategic culture then moves on to a discussion of the elements comprising it. These elements, which can also be identified in the cyber environment, include a sense of vulnerability, the narrative of Russia as a besieged fortress, and Russia´s technological inferiority. Methodologically, Article V is a literature survey, based on official

Russian documents related to information security. Article V answers research questions:

- What is Russia's cyber threat perception?
- How Russia is responding to this cyber threat?

The keywords of the Article V are culture theory, Russian strategic culture and Russian cyber threat perception.

Findings

The findings of Article V discuss the protection of Russia against cyber threats. The most important actions are the preparations to isolate RuNet from the global Internet, improved protection of the CIIRF, intensified surveillance of RuNet, the ban of user anonymity on RuNet, and the aspiration to replace imported ICT with Russian produced ICT.

The Russian assessment of the cyber threat contains the same besieged fortress narrative as in the country's other threat assessments. Hostile state and non-state actors are surrounding Russia in cyberspace and cyber threats against Russia are increasing and becoming more diverse. To protect itself against these cyber threats, Russia has taken operational, technical, and legal actions.

Russia is increasing its digital sovereignty by preparing technical and operational readiness to isolate RuNet from the global Internet. It is possible that Russia will manage to create technical and operational readiness to isolate RuNet from the global Internet at the end of 2020. Russia is also improving the protection of its critical information infrastructure. The definition of the CIIRF and the division of responsibilities between authorities to protect the CIIRF were confirmed by legislation in 2017 and the implementation phase has now started. The National Coordination Center for Computer Incidents (NCCCI) and part of the regional and territorial IS operations centers are operational.

Russia is lagging behind the leading foreign countries in the development of competitive information technology. This gap strengthens the Russian perception of its strategic vulnerability in cyberspace. For almost twenty years, Russia has tried, without success, to replace imported ICT software with Russian-made counterparts, and it seems that they will not succeed in the near future either.

Summary and the relation to the whole

Article V discusses Russia's defense against the cyber threats described in Article IV. After the introduction, Article V presents a description of Russian cyber threat perception. The main section of the Article discusses Russia's response to this threat. Grounded theory is used because little theoretical and structured information has, to date, been published on the Russian response to cyber threats. The data are drawn from official Russian documents such as strategies, doctrines, laws, and presidential decrees. Article V updates the cyber threat perception and especially Russia's response to that threat discussed in Article I. Article V also expands the discussion about threat picture and the response to those threats beyond the discussion in Articles II and III, which both concentrated on critical information infrastructure.

6.6 Article VI: Theory of Strategic Culture: An Analytical Framework for Russian Cyber Threat Perception

Kari, M and Pynnöniemi, K (2019). Theory of Strategic Culture: an Analytical Framework for Russian Cyber Threat Perception. Submitted to Journal of Strategic Studies in January 2019

Research objectives

Article VI is the theoretical framework of the thesis. It answers research question "How does Russian strategic culture explain Russia's cyber threat perception and its response to that threat?" The strategic environment is evolving rapidly with the recognition of cyberspace as a domain of warfare. The increased interest in cyber as a part of defense has heightened the need for theoretical tools suitable to assess cyber threat perceptions and responses to cyber threats. Article VI seeks to contribute to this effort by revitalizing strategic culture theory, which was originally developed for analysing the factors that influence strategic decision-making.

Article VI argues that the theory of strategic culture is suitable to explore and explain the formation of Russian cyber threat perceptions and the country's subsequent cyber strategy. The Article identifies specific factors influencing Russian strategic culture and discusses elements that comprise it. The latter include a sense of vulnerability, the narrative of Russia as a besieged fortress and the technological inferiority of Russia. These elements can also be identified in Russian cyber threat perception, which is discussed at the end of the Article. The keywords of Article VI are theory of strategic culture, Russia, cyber threats, cyberspace, and nature of the conflict.

Findings

The interest in cyber warfare has created a need for theoretical tools to research cyber threats and the responses to cyber threats. As this paper argues, the theory of strategic culture is a suitable tool to explore and explain the formation of Russian cyber threat perception. The theory of strategic culture tries to identify the factors that are characteristic for national decision-making and state practice and to study how and why these factors influence such decisions and practices. Factors with an influence on Russian strategic thinking include historical, geopolitical, religious or ideological ones. Elements of Russian strategic culture, such as a sense of vulnerability, the narrative of Russia as a besieged fortress, the mythology of permanent war, and technological inferiority can also be identified in Russian cyber threat perception.

The theory of strategic culture can also be used to explore and to explain Russian defensive cyber operations, based on its cyber threat perception, as well as the country's offensive cyber operations, such as cyber-attacks and cyber espionage. Elements of Russian strategic culture related to these operations include asymmetric means of warfare and the denial, deception and concept of tactical truth.

Summary and the relation to the whole

Article VI comprise the theoretical background of this thesis. It argues that the theory of strategic culture is suitable to explore and explain the formation of Russian cyber threat perceptions and the country's subsequent cyber strategy. The Article formulates an analytical framework to study the formation of Russian thinking on cyber threats as a part of Russian strategic culture. The Article identifies specific factors influencing Russian strategic culture and discusses elements that comprise it. The latter include a sense of vulnerability, the narrative of Russia as a besieged fortress and the technological inferiority of Russia. These elements can also be identified in the Russian cyber threat perception, which is discussed at the end of the Article.

7 CONCLUSIONS

Russian strategic culture can be used to explain Russian cyber threat perception and the country's response to cyber threats. The central paradigm of Russian strategic culture, which includes a sense of vulnerability, the concept of permanent war and the narrative of the besieged fortress, a Clausewitzian belief in the use of force, and a fear of external and internal enemies, can also be identified in the Russian cyber threat perception. NATO and the West are creating that threat in cyberspace as well.

Russia's methods to respond to cyber threats, that is, the strategic preferences of Russian strategic culture in cyberspace, are pivoting to international cyber security agreements, improving the protection of critical information infrastructure, and preparing to isolate the Russian segment of Internet from the global Internet. Russian armed forces and certain state authorities have their own communication networks, isolated totally or partly from Internet. Surveillance and censorship has increased and user anonymity has been banned on the Russian Internet. Russia is also trying to replace ICT imports from the West with technology produced in Russia.

The evolution of Russian cyber threat perception can be divided into three phases. The first phase, the phase of the relatively uncontrolled Russian segment of the Internet starting in the 1990s, ended after the demonstrations against election results and transfer of power from Medvedev to Putin in 2011 and 2012. Before that, the Kremlin, which had to that point concentrated on controlled TV channels, failed to realize the power of the Internet to spread information which was not supporting the official views and to call people to participate in demonstrations. In the first phase Russian authorities, especially the Federation Security Service (FSB), controlled Internet traffic through SORM systems, but a large portion of the so-called operative investigation measures concentrated on criminality and only a smaller part on surveillance of the opposition.

The severity of cyber threats was not realized and the roles and responsibilities of different authorities and agencies was not defined. For example, the list of protected objects in information space presented in ISD 2000, meaning the most important objects to protect, is broad and almost all-encompassing, including economics, domestic policy, foreign policy science and technology, spiritual life, information and telecommunication systems, defense, law enforcement and judicial spheres, and emergencies.

The concept of the critical information infrastructure of the Russian Federation (CIIRF) was officially discussed for the first time in ISD 2000, but ISD 2000 did not clearly and unambiguously describe the ideas of protecting the CIIRF and the responsibilities and division of labor between state authorities. To define and organize the protection of the CIIRF took almost two decades because of the power struggle over IS management between the FSB, the Federal Service for Technical and Export Control (FSTEC) and the Russian Armed Forces, and because of the clarification of the responsibilities of private companies and other legal entities for protection. The Law on the Protection of the CIIRF, which ended this power struggle, was passed in 2017.

The second phase of the Russian cyber treat perception began after 2012. This phase concentrated on controlling information content and flow, and responded mainly to information-psychological threats on the Internet, but responses to cyber threats were also discussed. The measures of Russian leadership to respond to information threats were increasing censorship, a pivot to a ban of anonymity in the Russian segment of the Internet and increased surveillance of Internet traffic. The main target of the response in the second phase was Russian opposition, but cyber defense against external threats was also improved. The Black List Law (FZ-139, 2012) and two laws in 2013 (FZ-135, 2013; FZ-398, 2013) gave Roskomnadzor, in practice, unlimited possibilities to block unwanted webpages. This mandate has been used to block opposition websites defined as extremist information by the Russian authorities.

Improving the identification of Internet users was one of the measures to control the opposition. In 2014, the Blogger Law obliged bloggers with more than 3,000 daily readers to be registered in Roskomnadzor and required so-called organizers of distribution of information on the Internet to store user data for six months in Russia as well as to disclose information to law enforcement authorities. The Armed Forces joined the conversation on cyber threats and cyber defense by publishing its Conceptual Views on the Activity of the Armed Forces in Information Space (2011).

Information struggle and information threats were mentioned in the Military Doctrine 2010, but cyberspace became a domain of permanent warfare in Russian threat perception after the annexation of Crimea in spring 2014. This third phase of the Russian cyber threat perception started concurrently with the annexation of Crimea and the outbreak of war in eastern Ukraine. In this third phase, Russia updated security-related documentation, such as the Military Doctrine (2014), National Security Strategy (2015), and Information Security Doctrine (2016). Control of users in the Russian segment of the Internet was increased by laws related to Roskomnadzor's mandate to block websites that included information unwanted by Russian leadership, with obligations to telecom operators to identify all their users and with a ban of anonymizers and virtual private networks.

The focus of the struggle against cyber threats was shifted from internal threats to external threats as a part of the general threat situation. The defense against external cyber threats was constructed from different layers, so-called perimeters, following the principle of defense in depth. Disagreements on the protection of the CIIRF and power over the responsibilities of state agencies were resolved, and the Law on the Protection of the CIIRF was passed in 2017. The system of CIIRF protection constructed the inner perimeter of defense against external cyber threats. The FSB was mandated to surveil cyber-attacks and protect objects of the CIIRF.

The owners of CIIRF objects were obliged to protect their objects in a manner defined in the law. The objects of CIIRF are information systems, information and telecommunication networks, and the automated control systems of technological processes operating in industries such as defense, fuel, nuclear, mining, metallurgical, chemical, rocket, space, healthcare, transport and communications. The outer defense perimeter against cyber threats is based on the idea of isolating the Russian segment of the Internet from the global Internet and minimizing the amount of Internet traffic crossing the Russian borders. The RuNet Law (FZ-90, 2019) obliged Internet operators to install technical equipment on their networks to counter threats to the functioning of the Russian segment of the Internet, a so-called kill switch by which the Russian Internet can be isolated from the global Internet. Through this equipment, Roskomnadzor can block prohibited Internet resources, including Telegram Messenger and VPN services. According to RuNet Law Russia will create its own autonomous DNS no later than the end of 2020.

Russian Internet traffic crossing Russian borders is transferred through registered Internet exchange points (IX points) and the traffic between the Russian segment of the Internet and the global Internet can be monitored. In addition the connection can be cut at these IX points (FZ-90, 2019). Isolating the Russian segment of the Internet is publicly justified as defense against external cyber threats, but the RuNet Law in practice increases the possibilities of Russian authorities to surveil internal opposition. The Russian Armed Forces and part of the state administration have their own communication networks, which are partly or totally isolated from the Russian segment of Internet as an extra layer or perimeter of protection.

Russian strategic culture, led by an elite consisting of representatives of security structures will probably not change in the coming five to ten years. This means that Russian cyber threat perception will remain the same and Russia will continue to increase its digital sovereignty. It is possible that Russia will manage to create technical and operational readiness to isolate the Russian segment of the Internet from the global Internet by the end of 2020. Russia is also improving the protection of its critical information infrastructure. The definition of the CIIRF and the division of responsibilities between authorities to protect it were confirmed by legislation in 2017 and the implementation phase has now started.

Russia has tried to establish an international treaty or code of conduct to prevent the use of information technology for military, terrorist or criminal purposes in cyberspace. Russia has disagreed with the reports by the United Nations Group of Governmental Experts (GGE) and the work of GGE will continue as led by Western states. Russia is currently attempting to set up the treaty or code of conduct as a result of Open-Ended Working Group (OEWG). Russia's plans to draft a regulatory international agreement on the sovereign right of states to determine information, technological and economic policies in the national segments of the Internet no later than March 2020 will probably not be realized.

For Russia, the most difficult question in responding to cyber threats is that the country is lagging behind the leading foreign countries in the development of competitive information technology, including supercomputers, and this gap strengthens the Russian perception of its strategic vulnerability in cyberspace. For almost twenty years, Russia has tried, without success, to replace imported ICT software with Russian-made counterparts, and it seems that they will not succeed in the near future either. It seems probable that Russia will not manage to substitute imported ICT in the near future, because there has not been improvement in Russian ICT research and development or production.

This thesis reveals a possible link between Russian defensive and offensive cyber activity. The data contained some indicators (objects of cyber threats) described in the Russian threat perception which are mirror images of the targets of Russian offensive cyberspace operations. In addition, Russian offensive cyber capabilities are developed to influence these targets. One thing which implies this connection is that the national election system was the first object on the list of the CIO Bill 2006, but it has not been mentioned since.

8 CONTRIBUTIONS, LIMITATIONS AND FURTHER STUDY

8.1 Contributions

This thesis is combination of information system science, international law, history, international politics, Russian studies and military sciences. The study has required that the researcher possess good knowledge of Russian, because the primary data are available in Russian. The contributions of this thesis have both academic and practical value. This thesis demonstrated how the research methods or theories of two different academic fields – grounded theory as a systematic methodology in the social sciences and the theory of strategic culture from field of international relations and politics – can be used in information system science and computer science studies. Grounded theory was used to collect and analyze the data and to structure the model of Russian cyber threat perception.

The theory of strategic culture was used to explore and explain this model. This thesis demonstrated that the theory of strategic culture explains Russian cyber threat perception in depth, because it takes into account elements of Russian general threat perception and the factors influencing Russian threat perception which apply in cyberspace as well. For example, the Russian pivot to isolate the Russian segment of the Internet is typically explained by the threat caused by the USA. As the reason for increased surveillance of the Internet in Russia is named the need for surveillance of the opposition. The use of Russian strategic culture expands and deepens these explanations by describing factors and elements of Russian strategic culture. For example, the threat perception caused by the USA can be explained by the narrative of the besieged fortress, the concept of permanent war and the so-called Barbarossa Syndrome, which all cause the sense of vulnerability. This sense of vulnerability is bolstered by technical arrearage. The need to surveil the opposition can be explained by the fear of internal enemies, which can be explained by the revolts and other internal events in Russian history which challenged the existence or state order of Russia. The Arab Spring at the beginning of the 2010s increased this threat perception.

Strategic culture offers insights into the threat perception of certain states. It can offer limited predictability about the state policy options to fight these threats and explain threat perception and response (Libel, 2016; Hoffman, 2017). At the practical level, this thesis collects, structures and analyzes information on Russian cyber threat perception and Russian cyber defense from different documents. It should be noted that the information on the actual Russian cyber threat perception and cyber defense objects, subjects and the tactics, techniques and procedures used to protect Russia against offensive cyberspace operations is restricted or secret. Yet the picture constructed in this thesis can be considered to reflect the real Russian cyber threat perception.

Russian strategies and doctrines on security policy and legislation, orders and guidance documents of different state authorities such as the FSB and the FSTEC on information management and cyber security provide Russian authorities, business, industry and society information on cyber threats and normative and legislative guidance to fight against cyber threats. This means that even if one law or other document on Russian cyber threat perception does not contain a lot of information, there is enough information scattered in official documents to construct a model of the country's real perception of cyber threats.

8.2 Limitations

Certain limitations and constraints need to be taken into consideration when evaluating and assessing the results of this research. These limitations also offer a framework and starting point for further research of topics related to Russian information management and cyber defense.

First, grounded theory was selected because it is well suited for studying a phenomenon about which there is a lack of theoretical and structured information, yet which would be needed to support professional decision-making or basic research. This thesis adopts the version of grounded theory developed by Anselm Strauss and Juliet Corbin because it accepts that the researcher is already familiar with the theoretical literature related to the area being studied. As the author of this thesis, I have familiarized myself with the theoretical literature related to the area during my professional career and during the process of completing my master's thesis.

Grounded theory was used in this thesis as a tool and a method to construct the model, the perspective and the pattern on Russian cyber threat perception and Russia's response to that threat. Grounded theory was not used to explain the factors behind Russian cyber threat perception. In this thesis, this Russian cyber threat picture and Russian cyber defense were then explained by the theory of strategic culture. The version of the theory of strategic culture used in this research is that developed by Alastair Iain Johnston. Even though Johnston's analytical framework is almost 25 years old, it remains valid. The central paradigm of Russian strategic culture corresponds to Russian threat perception and strategic preferences correspond to Russia's response to threats. This applies in cyberspace as well.

According to Johnston (1995b), one productive way to identify a central paradigm and strategic preferences is to analyse the content of recent texts related to the subject in question. The central paradigm of Russian strategic culture can be observed in subject-related high-level documents, such as strategies and doctrines. Strategic preferences, meaning tactics, techniques and procedures, can be found in doctrines and more practical documents, such as laws and guidance documents of different security-related state organizations. Because the researcher does not have insight on the implementation of strategic preferences in practice, this implementation had to be exposed and explained by describing the content of lower-level cyber related documents.

Furthermore, this thesis has also examined Russian information-technical threat perception and the Russian response to that threat. The information psychological part of information security was not discussed.

8.3 Further Study

8.3.1 Russian Cyber Threat Perception

Recently, there has been growing interest for studies of cyberspace as a domain of warfare. This has also caused the need for theoretical studies to estimate cyber threat perceptions of different states and the responses to cyber threats at a strategic level. Both the research process and results call for future studies. The evolution of Russian cyber threat perception and Russia's response to that threat should be under permanent study, because they continue to evolve. Even the legal basics of the protection of Russian critical information infrastructure, and the mandate for state security authorities for the protection of the Russian segment of the Internet are regulated in legislation, because the implementation of these laws remains incomplete.

Russian cyber threat perception is a part of the Russian general threat perception. Russian threat perception, which has an influence on Russian cyber threat perception, can be explained by using the theory of strategic culture. Strategic culture can change, and this change has influence to threat picture, including cyber threat picture. One area of future research could be to explore and explain, using the theory of strategic culture, the possible change in Russian cyber threat perception since Russia was established in 1991.

8.3.2 Russian Information Threat Perception

Information warfare can be information-technical, when informational-technical systems are objects of influence in cyberspace, or information-psychological, when the adversary tries to influence a person's mind, his or her moral and mental world, social and political opinions, and ability to make decisions (Kamyshev 2009). This thesis has studied Russian information-technical threat perception and the Russian response to that threat. An interesting area for further research is Russian information-psychological threat perception and Russia's response to that threat. Another interesting research approach is to study Russian information threat perception, which includes both information-technical and information-psychological components.

8.3.3 Russian Offensive Cyber Capabilities and Operations

The confrontation between Russia and the West is expanding from the real world to cyberspace. Especially during the last decade, Russia has been accused of being one of the main actors in a variety of cyberspace espionage and sabotage operations. There has been a lot of information about alleged Russian cyber espionage operations, starting from 2008 "Operation Buckshot Yankee" (Shactman, 2010) to the latest accusations, in spring 2018, by the UK and the USA, that Russia has "escalated the cyber war by espionage, stealing intellectual property and laying the foundation for an attack on infrastructure" (MacAskill, 2018). In addition to accusations of cyber espionage, Russia has been accused of cyberattacks in, for example, Estonia in 2007, Georgia in 2008 and repeatedly in Ukraine since 2014, when the war in eastern-Ukraine broke out (Connell & Vogler, 2017).

Russian offensive cyberspace activities are an interesting area. One research approach could start with the hypothesis that the objects of cyber threat described in the Russian threat perception are a mirror image of the targets of Russian offensive cyberspace operations. The tactics, techniques and procedures used by attacker can be also be mirror image for those of Russian offensive cyberspace operations. One thing, which implies to this, is the fact that the Russian State Election System was the first object on the list of the draft of the law on protection of critical information infrastructure 2006, but has not been mentioned since that time.

Another hypothesis could be that Russian offensive cyber capabilities are now under development to achieve the performance of these Western tactics, techniques and procedures. Figure 17 presents the idea of using Russian cyber threat perception as a mirror image of Russian offensive cyber capabilities.

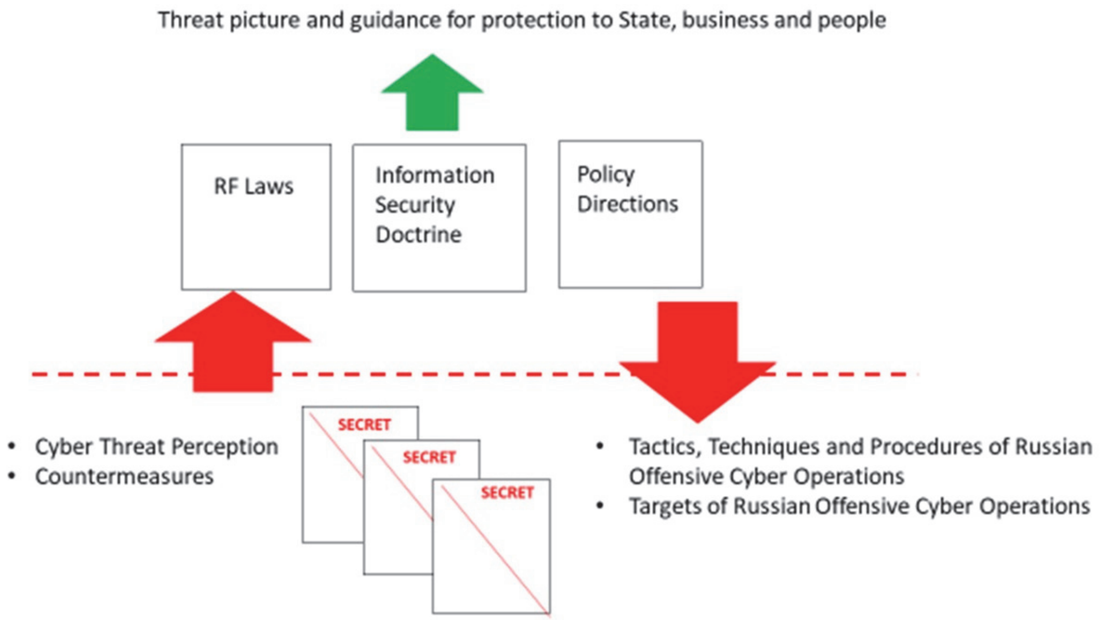

Threat picture and guidance for protection to State, business and people
RF Laws
Information Security Doctrine
Policy Directions
• Cyber Threat Perception
• Countermeasures
SECRET
SECRET
SECRET
• Tactics, Techniques and Procedures of Russian Offensive Cyber Operations
• Targets of Russian Offensive Cyber Operations

FIGURE 17 Russian Cyber Threat Perception as a Mirror Image of Offensive Cyber Capabilities

A challenge in the research of Russian offensive cyberspace activity is that there is not similar primary data available publicly on offensive cyberspace activities as there is on defensive cyberspace activities. The central paradigm of offensive cyberspace activities that is, the perception of warfare, the enemy and the threat – can be found in strategies and doctrine, but information on the strategic preferences of offensive cyberspace activities is difficult to find, because no equivalent legislation and directives are publicly available.

8.4 Other Topics of Further Study

Two more specific topics of further study are the development and production of Russian ICT, namely, the hardware and software intended to replace ICT imported from the West and China. Another topic might be Russia's aspirations and activities in international forums to create a generally accepted agreement, code of conduct or other binding document of international law regulating state behaviour in cyberspace.

SUMMARY

Lisääntynyt kiinnostus kybertoimintaympäristöön kansainvälisen politiikan areenana on lisännyt myös tarvetta tutkimuksellisiin menetelmiin, joiden avulla voidaan arvioida eri valtioiden kokemaan kyberuhkaa ja kyberuhkan torjuntaa. Venäjän kokemasta kyberuhkasta on julkaistu vähän tutkittua tietoa. Venäläisissä julkisissa asiakirjoissa kuitenkin on riittävästi informaatiota, jonka perusteella pystyy muodostamaan kuvan venäläisten kokemasta kyberuhkasta. Tässä kuudesta artikkelista koostuvassa väitöskirjassa selvitettiin Venäjän kokemaa kyberuhkaa ja sitä, miten Venäjä pyrkii torjumaan kyberuhkia. Tämä väitöskirjatutkimus osoittaa, että oikein valituilla ja käytetyillä menetelmillä ja lähdeaineistolla on mahdollista rakentaa ja selittää malli Venäjän kokemasta kyberuhkasta ja keinoista, joilla Venäjä pyrkii torjumaan kyberuhkaa.

Tutkimusprosessi koostui kolmesta vaiheesta. Metodina datan keräämisen ohjaamiseen ja Venäjän kokemaa kyberuhkaa kuvaavan mallin rakentamiseen käytettiin grounded theorya, jota käytetään laadullisessa tutkimuksessa yhteiskuntatieteiden alalla. Toisessa vaiheessa hahmotettiin strategisen kulttuurin teorian avulla Venäjän yleinen uhkakuva ja sen muodostumiseen vaikuttavat tekijät. Kolmannessa vaiheessa selitettiin strategisen kulttuurin teorian avulla mallia Venäjän kokemasta kyberuhkasta.

Strategisen kulttuurin teorian mukaan kullakin valtiolla on oma strateginen kulttuuri, mikä tarkoittaa valtion arviota sodan luonteesta, vastustajasta ja uhkasta sekä valtion keinoista vastata uhkaan. Aineistona on käytetty virallisia venäläisiä kyberturvallisuutta käsitteleviä asiakirjoja kuten strategioita, doktriineja, lakeja ja asetuksia. Väitöskirjaa varten koodattiin 140 venäläistä kansalliseen turvallisuuteen, kyberturvallisuuteen tai Venäjän digitalisointiin liittyvää asiakirjaa vuosilta 1995-2019. Koodaukseen käytettiin data-aineiston hallitsemiseen ja laadulliseen analyysiin tarkoitettua Atlas.ti ohjelmistoa.

Tutkimustuloksena aineistosta nousi kyberuhkan kohteiksi Venäjän strategisen tasan kansalliset intressit, informaatio, informaatioinfrastruktuuri ja Venäjän asevoimat. Venäläinen kyberuhkakuva heijastaa kiristynyttä kansainvälistä tilannetta. Siinä näkyvät yllätyshyökkäyksen kohteeksi joutumisen pelko, kertomus Venäjästä piiritettynä linnakkeena, venäläinen ajatus sodan ja rauhan väliin sijoittuvasta jatkuvasta sodankäynnistä ja voimankäyttö yhtenä ulkopolitiikan menetelmänä. Sisäisten vihollisten uhka on kasvanut viime vuosina. Venäläisten huoli omasta teknologisesta jälkeenjääneisyydestään informaatioteknologian alalla tuli hyvin tutkimuksessa esille.

Venäjän tärkeimmät toimenpiteet kyberuhkan torjunnassa ovat pyrkimys luoda kyky Internetin venäläisen segmentin irrottamiseen tarvittaessa globaalista internetistä, Venäjän kriittisen informaatioinfrastruktuurin suojaamisen kehittäminen, Venäjän sisäisen ja Venäjän rajat ylittävän verkkoliikenteen valvonnan tehostaminen, anonyymien käyttäjien kielto ja yritykset korvata ulkomaiset ICT-laitteet ja tietokoneohjelmistot venäläisvalmisteisilla tuotteilla.

REFERENCES

Adamsky, D. 2018. 'Cultural Underpinnings of Current Russian Nuclear and Security Strategy', in Johnson J.L., Kerry Kartchner and Marilyn Maines (eds) *Crossing Nuclear Thresholds. Leveraging Sociocultural Insights into Nuclear Decisionmaking.* New York: Palgrave Macmillan.

Almond, G. & Verba, S. 1963. *The Civic Culture: Political Attitudes and Democracy in Five Nations.* Princeton: Sage Publications Inc.

APIS. 2017. План мероприятий по направлению "Информационная безопасность" программы "Цифровая экономика Российской Федерации". [Action plan of "Information Security" of the program "Digital Economy of the Russian Federation".] http://static.government.ru/media/files/AEO92iUpNPX7Aaonq34q6BxpAHCY2umQ.pdf

Aron, L. 2008. The Problematic Pages. In memory of Alexander Solzhenitsyn. *The New Republic*. https://newrepublic.com/article/62070/the-problematic-pages

Babchuk, W. 1996. Grounded Theory as a "Family of Methods": A Genealogical Analysis to Guide Research. *US-China Education Review* A 3, 383-388. https://pdfs.semanticscholar.org/8064/c652f4efa1c1e23f3beb33a143abd3683c4d.pdf

Baskerville, R. 1993. Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR)*. 25(4), 375-414 DOI: 10.1145/162124.162127

Berrett, M. & Johnson, J. 2011. "Cultural Topography: A New Research Tool for Intelligence Analysis — Central Intelligence Agency." *CIA Library*. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-2/cultural-topography-a-new-research-tool-for-intelligence-analysis.html

Bloomfield, A. 2012. ´Time to Move On: Reconceptualizing the Strategic Culture Debate.` *Contemporary Security Policy,* 33 (3), 437-461. https://www.tandfonline.com/doi/abs/10.1080/13523260.2012.727679

Birks, M. & Mills, J. 2015. *Grounded Theory. A practical Guide.* London: Sage.

Bolden, M. & Nalla, M. 2014. Theorizing Cybercrime: Applying Routine Activities Theory. https://www.academia.edu/8897451/Theorizing_Cybercrime_Applying_Routine_Activities_Theory

Booth, K. 2005. Strategic Culture: Validity and Validation. *Oxford Journal on Good Governance*, 2 (1), 25-28. http://ocgg.org/fileadmin/Journal/OJGG_Vol_2_No_1.pdf

Brusnitsin, N. 2000. Кто *подслушивает президентов* (От *Сталина до Ельцина*). [Who is wiretapping the presidents (From Stalin to Yeltsin).] Moscow : Вита-Пресс.

Charmaz, K. 2014. *Constructing Grunded Theory. A Practical Guide Through Qualitative Analysis.* London: SAGE.

CICT. 2019. Центр компетенций по импортозамещению в сфере информационно-коммуникационных технологий (ЦКИКТ). [Competence Center for Import Substitution in Information and Communication Technologies (CICT).] http://ru-ikt.ru/about/

Cimbala, S. 2013. Russian Threat Perceptions and Security Policies: Soviet Shadows and Contemporary Challenges. *The Journal of Power Institutions in Post-Soviet Societies*. 14/15 https://journals.openedition.org/pipss/4000

Cirenza, P. 2016. The Flawed Analogy Between Nuclear and Cyber Deterrence. *Bulletin of the Atomic Scientists.* http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179

Clausewitz, C. 1832. Vom Kriege. Helsinki: Art House. (1988).

Connell, M. & Vogler, S. 2017. Russia's Approach to Cyber Warfare. *CNA Corporation*. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf

Cooney, A. 2010. Choosing between Glaser and Strauss: an examples. *Nurse Researcher*. 17 (4), 18-28. https://europepmc.org/abstract/med/20712231

Corbin, J. & Strauss, A. 1990. Grounded Theory Research: Procedures, Canons, and Evaluative Criteria. *Qualitative Sociology*, 13 (1), 3-21.

Corbin, J. & Strauss, A. 2008. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory (3rd ed.).*, Thousand Oaks, CA: Sage.

Covington, S. 2016. The Culture of Strategic Thought Behind Russia's Modern Approaches to Warfare. *Belfer Center. Harvard Kennedy School.* https://www.belfercenter.org/sites/default/files/files/publication/Culture%20of%20Strategic%20Thought%203.pdf

CRC. 2016. Cyberspace: the Fifth Domain of War!? *Cyber Research Center – Industrial Control Systems.* https://www.crc-ics.net/documents/CRC-ICS-2016_Cyber-Space_the_fith_domain_of_war_2016-v2.6.pdf

Davis Cross, M. 2013. ´Rethinking epistemic communities twenty years later.` *Review of International Studies*, 39 (1), 137-160. https://doi.org/10.1017/S0260210512000034

Demidov, O. 2013. Киберкомандование США: уроки для России. [The US Cyber command: Lessons to Russia.] http://www.perspektivy.info/rus/konturi/kiberkomandovanije_ssha_uroki_dla_rossii_2013-11-15.html

Desch, M. 1998. Culture Clash: Assessing the Importance of Ideas in Security Studies. *International Security,* 23 (1), 141-170.

Dey, I. 2001. Grounded Theory. C. Seale, G. Gobo, J. Gubrium, D. Silverman, (ed.) *Qualitative Research Practice*. London: SAGE.

Drew, J. 2018. Space, Cyber and Changing Notions of War. *Small War Journal.* https://smallwarsjournal.com/jrnl/art/space-cyber-and-changing-notions-of-war

ECCWS. 2019. 18th European Conference on Cyber Warfare and Security, 4 - 5 July 2019, University of Coimbra, Portugal. https://www.academic-conferences.org/conferences/eccws/

Echevarria II, A. 2017. ´Strategic Culture is not a Silver Bullet.` *Naval War College Review*, 70 (4). https://digital-commons.usnwc.edu/nwc-review/vol70/iss4/8

Eitelhuber, N. 2009. The Russian Bear: Russian Strategic Culture and What it Implies for the West. https://procon.bg/system/files/09.1.01_Eitelhuber.pdf

Eliseev, I. 2013. Забил я цифрой пушку туго. Помогут ли победе в информационной войне роботы и мобилизация хакеров? [I shot with the digital cannon. Will robots and hacker mobilization help win the information war?] *Rossiyskaya Gazeta,* 6085 (109). https://rg.ru/2013/05/23/ashmanov.html

Ermarth, Fritz. 2006. Russian Strategic Culture: Past, Present, and… in Transition? *Defense Threat Reduction Agency Advanced Systems and Concepts Office.* https://fas.org/irp/agency/dod/dtra/russia.pdf

Facon, I. 2016. « Russian Strategic Culture in the 21st Century: Redefining the West-East Balance », in Ashley J. Tellis, Alison Szalwinski, Michael Wills (ed.), *« Understanding Strategic Cultures in the Asia-Pacific », Strategic Asia 2016-2017*, The National Bureau of Asian Research, 62-89. http://nbr.org/publications/strategic_asia/pdf/SA16_ExecutiveBrief.pdf

Facon, I. 2017. Russia's national security strategy and military doctrine and their implications for the EU. *European Parliament's Sub-Committee on Security and Defence.* http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/578016/EXPO_IDA(2017)578016_EN.pdf

Felgenhauer, P. 2005. Russia's Imperial General Staff. *Perspective*, XVI (1). https://www.bu.edu/iscip/vol16/felgenhauer.html

FZ-1. 2013. Федеральный закон о безопасности критической информационной инфраструктуры Российской Федерации - проект. [Proposal for the federal law on the security of critical information infrastructure.] http://rg.ru/pril/article/83/27/52/zakonoproekt.doc

FZ-5. 1996. Федеральный закон от 10 января 1996 г. N 5-ФЗ "О внешней разведке". [Federal law of January 10, 1996 N 5-FZ "On foreign intelligence".] http://www.kremlin.ru/acts/bank

FZ-40. 1995. Федеральный закон "О федеральной службе безопасности" от 03.04.1995 N 40-ФЗ. [Federal Law "On the Federal Security Service" of 03.04.1995 N 40-FZ.] http://www.consultant.ru/document/cons_doc_LAW_6300/

FZ-61. 1996. Федеральный закон от 31 мая 1996 г. N 61-ФЗ г. Москва "Об обороне". [Federal Law of May 31, 1996, N 61-FZ, Moscow "On Defense".] http://rg.ru/1996/06/06/oborona-dok.html

FZ-90. 2019. Федеральный закон от 1 мая 2019 г. N 90-ФЗ "О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации". [Federal Law of 1 May, 2019 N 90-ФЗ "On amendments to the Federal Law" On Communications "and the Federal Law" On

Information, Information Technologies and Information Protection ".] https://rg.ru/2019/05/07/fz90-dok.html

FZ-97. 2014. Федеральный закон "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей" от 05.05.2014 N 97-ФЗ. [Federal Law "On Amendments to the Federal Law" On Information, Information Technologies and Information Protection" and certain legislative acts of the Russian Federation on the streamlining of information exchange using information and telecommunication networks" dated 05.05.2014 N 97-FZ.] https://rg.ru/2014/05/07/informtech-dok.html

FZ-102. 2018. Федеральный закон "О внесении изменений в Федеральный закон "Об исполнительном производстве" и статью 15.1 Федерального закона "Об информации, информационных технологиях и о защите информации" от 23.04.2018 N 102-ФЗ. [Federal Law "On Amendments to the Federal Law" On Enforcement Proceedings "and Article 15.1 of the Federal Law"On Information, Information Technologies and Information Protection"of 04.23.2018 N 102-FZ.] https://rg.ru/2018/04/25/fz102-dok.html

FZ-135. 2013. Федеральный закон от 29 июня 2013 г. N 135-ФЗ г. Москва "О внесении изменений в статью 5 Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации в целях защиты детей от информации, пропагандирующей отрицание традиционных семейных ценностей. [Federal Law of June 29, 2013 N 135-FZ Moscow "On Amendments to Article 5 of the Federal Law" On the Protection of Children from Information Harmful to their Health and Development "and certain legislative acts of the Russian Federation in order to protect children from information promoting the denial of traditional family values.] https://rg.ru/2013/06/30/deti-site-dok.html

FZ-139. 2012. Федеральный закон "О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации" от 28.07.2012 N 139-ФЗ. [Federal Law On Amendments to the Federal Law "On the Protection of Children from Information Harmful to Their Health and Development"and Certain Legislative Acts of the Russian Federation" of 28.07.2012 N 139-FZ.] https://rg.ru/2012/07/30/zakon-dok.html

FZ-144. 1995. Федеральный закон "Об оперативно-розыскной деятельности" от 12.08.1995 N 144-ФЗ. [Federal Law "On Operational-Search Activity" dated August 12, 1995 N 144-FZ.] https://legalacts.ru/doc/federalnyi-zakon-ot-12081995-n-144-fz-ob/

FZ-149. 2006. Федеральный закон от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации. [Federal Law of July 27, 2006 N 149-ФЗ On Information, Information Technologies and Information Protection.] https://rg.ru/2006/07/29/informacia-dok.html

FZ-152. 2006. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ. [Federal Law "On Personal Data" dated July 27, 2006 No. 152-FZ.] http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108261

FZ-172. 2014. Федеральный закон от 28 июня 2014 г. N 172-ФЗ "О стратегическом планировании в Российской Федерации". [Federal Law of June 28, 2014 N 172-FZ "On Strategic Planning in the Russian Federation".] https://rg.ru/2014/07/03/strategia-dok.html

FZ-187. 2017. Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации". [Federal Law of July 26, 2017 N 187-FZ “On the security of the critical information infrastructure of the Russian Federation”.] https://rg.ru/2017/07/31/bezopasnost-dok.html

FZ-241. 2017. Федеральный закон от 29 июля 2017 г. N 241-ФЗ "О внесении изменений в статьи 101 и 154 Федерального закона "Об информации, информационных технологиях и о защите информации". [Federal Law of July 29, 2017 N 241-ФЗ “On Amendments to Articles 101 and 154 of the Federal Law “On Information, Information Technologies and Information Protection”.] https://rg.ru/2017/08/04/informacia-dok.html

FZ-242. 2014. Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях" от 21.07.2014 N 242-ФЗ. [Federal Law "On Amendments to Certain Legislative Acts of the Russian Federation regarding the clarification of the procedure for processing personal data in information and telecommunication networks" dated July 21, 2014 N 242-FZ.] https://rg.ru/2014/07/23/persdannye-dok.html

FZ-245. 2017. Федеральный закон "О внесении изменений в Федеральный закон "О связи" от 29.07.2017 N 245-ФЗ. [Federal Law "On Amendments to the Federal Law" “On Communications "dated July 29, 2017 N 245-FZ.] https://rg.ru/2017/07/31/fz245-site-dok.html

FZ-276. 2017. Федеральный закон "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" от 29.07.2017 N 276-ФЗ. [Federal Law "On Amendments to the Federal Law" On Information, Information Technologies and Information Protection "of 29.7.2017 N 276-FZ.] https://rg.ru/2017/07/30/fz276-site-dok.html

FZ-327. 2017. Федеральный закон "О внесении изменений в статьи 10.4 и 15.3 Федерального закона "Об информации, информационных технологиях и о защите информации" и статью 6 Закона Российской Федерации "О средствах массовой информации" от 25.11.2017 N 327-

ФЗ. [The Federal Law "On Amendments to Articles 10.4 and 15.3 of the Federal Law" On Information, Information Technologies and Information Protection "and Article 6 of the Law of the Russian Federation" On Mass Media "dated November 25, 2017 N 327-FZ.] http://kremlin.ru/acts/bank/42487

FZ-374. 2016. Федеральный закон "О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности" от 06.07.2016 N 374-ФЗ. [Federal Law "On Amendments to the Federal Law" On Counter-Terrorism "and certain legislative acts of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety" of 07/07/2016 N 374-FZ.] https://rg.ru/2016/07/08/antiterror-dok.html

FZ-375. 2016. Федеральный закон "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности" от 06.07.2016 N 375-ФЗ. [Federal Law "On Amendments to the Criminal Code of the Russian Federation and the Criminal Procedure Code of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety" dated July 06, 2016 N 375-FZ.] https://rg.ru/2016/07/11/uk375-dok.html

FZ-398. 2013. Федеральный закон "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" от 28.12.2013 N 398-ФЗ. [Federal Law "On Amendments to the Federal Law "On Information, Information Technologies and Information Protection" of 12/28/2013 N 398-FZ.] http://www.consultant.ru/document/cons_doc_LAW_156518/

FZ-4524. 1993. Закон РФ "О федеральных органах правительственной связи и информации" от 19.02.1993 N 4524-*1*. [Law of the Russian Federation "On Federal Government Communications and Information" dated February 19, 1993 N 4524-1.] http://zakonbase.ru/content/part/138824

FZ-5485. 1993. Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1. [Law of the Russian Federation "On State Secrets" of July 21, 1993 N 5485-1.] http://www.consultant.ru/document/cons_doc_LAW_2481/

FZP-340741-4. 2006. Федеральный закон об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры. Законопроект отклонен. [Federal law on the specifics of ensuring information security of critical objects of the information and telecommunications infrastructure. Bill rejected.] http://xn----9sbmabrf5adsldy9e3b.xn--p1ai/bill/340741-4

FZP-47571-7. 2017. Федеральный закон о безопасности критической информационной инфраструктуры Российской Федерации - проект.

[Federal law on the security of the critical information infrastructure of the Russian Federation - draft.] http://asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=475717

FZP-608767-7. 2018. О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации». [On amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and the Protection of Information".] http://www.lexfeed.ru/law/608767-7

Geers, K. & Czosseck, C. 2009. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Washington D.C.: IOS Press.

Geers, K. 2011. Strategic Cyber Security. Tallinn: CCDCOE. https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Geers.pdf

Geers, K. 2015. Cyber war in perspective: Russian aggression against Ukraine. Tallinn: CCDCOE. https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf

Gerasimov, V. 2013. Ценность науки в предвидении. Новые вызовы требуют переосмыслить формы и способы ведения боевых действий. [The value of science in anticipation. New challenges require rethinking the forms and methods of warfare.] *Военно-промышленный курьер*, 8 (476). https://www.vpk-news.ru/articles/14632

Giles, K. 2012. Russia's public stance on cyberspace issues. *4th International Conference on Cyber Conflict.* Tallinn: CCDCOE. http://www.conflictstudies.org.uk/files/Giles-Russia_Public_Stance.pdf

Giles, K. & Monaghan, A. 2013. Legality in Cyberspace: The Russian View. *Conflict Studies Research Centre.* https://ssi.armywarcollege.edu/pdffiles/PUB1193.pdf

Giles, K. & Monaghan, A. 2014. Legality in Cyberspace: An Adversary View. *The Letort Papers*. Strategic Studies Institute and U.S. Army War College Press. Carlisle

Giles, K. 2019. The Next Phase of Russian Information Warfare. *Conflict Studies Research Centre Ltd* https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles

Glaser, B. & Strauss, A. 1967. *The Discovery of Grounded Theory. Strategies for Qualitative Research*. Chicago: Aldine Publishing Company.

Glaser, B. 2011. *The grounded theory perspective: conceptualization contrasted with description*. Mill Valley, CA: Sociology Press.

Global Security (2014a). Federal Security Service (FSB). http://www.globalsecurity.org/intell/world/russia/fsb.htm

Global Security (2014b). Foreign Intelligence Service (SVR). http://www.globalsecurity.org/intell/world/russia/svr.htm

Gray, C. 1971. What Rand Hath Wrought. *Foreign Policy*, 4, 118.

Gray, C. 1999. Strategic Culture as Context: The First Generation of Theory Strikes Back. *Review of International Studies,* 25 (1), 49-69

Gray, C. 2006 "Out of the Wilderness: Prime-time for Strategic Culture," *inaugural speech made at the Defense Threat Reduction Agency (DTRA)* https://fas.org/irp/agency/dod/dtra/stratcult-out.pdf

Gusachenko, V. 2007. Об актуальном контексте поятия «национальная безопасность». [On the current context of the concept of national security.] *Военная Мысль*. 7, 2-13. http://militaryarticle.ru/voennaya-mysl/2007-vm/10032-ob-aktualnom-kontekste-ponjatija-nacionalnaja

Heritage Foudation. 1997. The "Primakov Doctrine": Russia's Zero Sum Game with the United States. https://www.heritage.org/report/the-primakov-doctrine-russias-zero-sum-game-the-united-states

Hoffman, F. 2017. Review Essay - Strategic Culture And Ways Of War, Elusive Fiction Or Essential Concept? *Naval War College Review,* 70 (2). https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1018&context=nwc-review

Horton-Eddison, M. 2018. Is Theory of Strategic Culture Valid?. https://www.academia.edu/12536463/Is_the_Theory_of_Strategic_Culture_Valid

Howlett, D. & Glenn, J . 2005. Nordic strategic culture. *Cooperation and Conflict*, 40 (1), 121–140. https://journals.sagepub.com/doi/10.1177/0010836705049737

ICCWS. 2019. 15th International Conference on Cyber Warfare and Security, 12 March- 13 March 2019, Norfolk, Virginia. https://www.academic-conferences.org/conferences/iccws/

Igumnova L. 2011. Russia's Strategic Culture Between American and European Worldviews. *The Journal of Slavic Military Studies*, 24 (2). http://www.tandfonline.com/doi/abs/10.1080/13518046.2011.572729

Interfax. 2018. За год на Россию было совершено более 4 млрд кибератак. Over the year, more than 4 billion cyberattacks were committed to Russia. https://www.interfax.ru/russia/641760

IT-Gov. 2018. What is Cyber Security? https://www.itgovernance.co.uk/what-is-cybersecurity

Jasper, S. 2017. *Strategic Cyber Deterrence*. New York: Rowman & Littlefield. 2017.

Jaishankar K. 2007. Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, 1 (2), 7-9. http://www.cybercrimejournal.com/Editoriaijccjuly.pdf

Johnston A. 1995a. Thinking about Strategic Culture. *International Security,* 19 (4), 32-64. http://www.fb03.uni-frankfurt.de/45431264/Johnston-1995-Thinking-about-Strategic-Culture.pdf

Johnston A. 1995b. *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*. Princeton:University Press.

JYU. 2019. Master's Degree Programme in Information Systems. University of

Jyväskylä. https://www.jyu.fi/ops/fi/it/masters-degree-programme-in-information-systems

Kamyshev, E. 2009. *Информационная безопасность и защита информации.* [Information Security and Protection of Information.] http://window.edu.ru/resource/033/75033/files/InfoBesop.pdf

Karlin, A. 2018. Russia's Technological Backwardness. *The UNZ Review*. http://www.unz.com/akarlin/russias-technological-backwardness/

Kelle, U. 2005. "Emergence" vs. "Forcing" of Empirical Data? A Crucial Problem of "Grounded Theory" Reconsidered. *Forum Qualitative Sozialforschung*. 6 (2). http://www.qualitative-research.net/index.php/fqs/article/view/467/1000http://journals

Kennan, G. 1947. The Sources of Soviet Conduct. *Foreign Affairs* 25, 566-82. https://is.muni.cz/el/1423/jaro2017/BSS185/um/Week_4_Kennan_on_Containment.pdf

Kerry, J. 2013. Hearing before the Committee on Foreign Relations of United States. https://www.gpo.gov/fdsys/pkg/CHRG-113shrg86451/pdf/CHRG-113shrg86451.pdf

Kenny, M. & Fourie, R. 2014. Tracing the History of Grounded Theory Methodology: From Formation to Fragmentation. *The Qualitative Report*, 19 (103), 1-9. http://www.nova.edu/ssss/QR/QR19/kenny103.pdf

Kolesnikov A. 2016. Do Russians Want War?. *Carnegie Moscow Center.* http://carnegieendowment.org/files/Article_Kolesnikov_2016_Eng-2.pdf

Komarov, A. 2016. Нормативные документы по безопасности АСУ ТП, АСУ ПиТП, КСИИ, КВО, КИИ. [Regulatory documents on safety of ASU TP, ASU PiTP, KSII, KVO, KII.] https://www.securitylab.ru/blog/personal/zlonov/144489.php

Koskennurmi-Sivonen, R. 2004. Grounded theory. https://rkosken.kapsi.fi/gt.html

Kukkola, J., Ristolainen M. & Nikkarila J-P. 2017. *Game Changer - Structural transformation of cyberspace*. Finnish Defence Research Agency Publications. https://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+julkaisuja+10.pdf/5d341704-816e-47be-b36d-cb1a0ccae398

Kukkola, J., Ristolainen M. & Nikkarila J-P. 2019. *Game Player- Facing the structural transformation of cyberspace*. Finnish Defence Research Agency Publications. https://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+julkaisuja+11+Game+Player.pdf/a4e38a00-e30e-cc48-f3af-d590655509ba/PVTUTKL+julkaisuja+11+Game+Player.pdf.pdf

Lantis, J. 2002. Strategic Culture and National Security Policy. http://www.fb03.uni-frankfurt.de/45431305/Lantis-2002--Strategic-Culture-and-National-Security-Policy.pdf

Lantis, J. 2006. Presentation on theme: "Strategic Culture and Threat Assessment”. *Second Annual Joint Threat Anticipation Center Workshop*. The University of Chicago. http://slideplayer.com/slide/4271931/

Lapina, M., Revin, A. & Lapin, V. *Informatsionnoe Pravo*. [Informational Law].

Moscow: Juniti-dana. Zakon i pravo.

Lavrentjeva, N. 2012. В России разработали государственную политику кибер-защиты. [Russia has developed a state cyber-defense policy.] http://www.cnews.ru/news/top/v_rossii_razrabotali_gosudarstvennuy

Libel, T. 2016. Explaining the security paradigm shift: strategic culture, epistemic communities, and Israel's changing national security policy, *Defence Studies*. DOI: 10.1080/14702436.2016.1165595

Lock, E. 2018. Strategic Culture Theory: What, Why, and How. http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-320#acrefore-9780190228637-e-320-div1-2

Lynch, A. 2002. The Evolution of Russian Foreign Policy in the 1990s. *Journal of Communist Studies and Transition Politics*, 18 (1), 161–182.

MacAskill, E. 2018. US and UK blame Russia for 'malicious' cyber-offensive. *The Guardian.* https://www.theguardian.com/technology/2018/apr/16/us-and-uk-blame-russia-for-malicious-cyber-offensive

Meduza. 2016. Russia's Communications Ministry plans to isolate the RuNet by 2020. https://meduza.io/en/news/2016/05/13/communications-ministry-plans-to-isolate-runet-by-2020

Millett, L., Fischhoff, B. & Weinberger, P. 2017. Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions. *National Academies of Sciences, Engineering, and Medicine, Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board.* Washington, DC: The National Academies Press. https://doi.org/10.17226/24676.

Moukin, G. 2013. Supercomputing Gap Seen as Threat to Economy. *The Moscow Times.* https://themoscowtimes.com/articles/supercomputing-gap-seen-as-threat-to-economy-29999

MDRF. 2010. Военная доктрина Российской Федерации. [Military doctrine of the Russian Federation.] http://rg.ru/2010/02/10/doktrina-dok.html

MDRF. 2011. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. [Conceptual views on the activities of the Armed Forces of the Russian Federation in the information space.] http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle

MDRF. 2014. Военная доктрина Российской Федерации. [Military doctrine of the Russian Federation.] http://www.scrf.gov.ru/documents/18/129.html

Monaghan, A. 2008. 'An enemy at the gates' or 'from victory to victory'? *Russian Foreign Policy.* http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2346.2008.00734.x/abstract

Murray, W. 1999. "Does Military Culture Matter?". *Orbis*, 43 (1), 27-42. https://doi.org/10.1016/S0030-4387(99)80055-6

Nato. 2016. Cyber Defence Pledge. *Press Release 2016*, 124.

https://www.nato.int/cps/en/natohq/official_texts_133177.htm

N&O Column. 2009. Intelligence profile: Russian Federation. http://www.cvni.net/radio/nsnl/nsnl145/nsnl145ru.html

Orlov V. 2011. Начало новых битв. [Start of new battles.] *Moskovskie Novosti*. http://www.mn.ru/newspaper/world/68636

Ovtsarenko Y. 2004. Заместитель главы администрации Президента РФ Владислав Сурков: Путин укрепляет государство, а не себя. [Deputy Head of the Presidential Administration Vladislav Surkov: Putin is strengthening the state, not himself.] https://www.kompravda.eu/daily/23370/32473/

Pape, R. 1996. *Bombing to Win: Air Power and Coercion in War*. Ithaca & London: Cornell University Press.

PFSB-366. 2018. Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 366 "О Национальном координационном центре по компьютерным инцидентам" [Order of the Federal Security Service of the Russian Federation of 24.07.2018 No. 366 "On the National Computer Incident Coordination Center"] http://publication.pravo.gov.ru/Document/View/0001201809100001

PFSO-443. 2016. Приказ ФСО России от 07.09.2016 N 443 "Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети "Интернет" (Зарегистрировано в Минюсте России 14.10.2016 N 44039). [Order of the Federal Protection Service of Russia of 07.09.2016 N 443 "On Approval of the Regulation on the Russian State Segment of the Internet Information and Telecommunication Network" (Registered in the Ministry of Justice of Russia 14.10.2016 N 44039)] https://minjust.consultant.ru/documents/21109?items=1&page=2

PFSO-487. 2009. Приказ ФСО РФ от 07.08.2009 N 487 "Об утверждении Положения о сегменте информационно-телекоммуникационной сети "Интернет" для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации" (Зарегистрировано в Минюсте РФ 04.09.2009 N 14705). [Order of the Federal Protection Service of the Russian Federation of 07.08.2009 N 487 "On approval of the Regulation on the segment of the information and telecommunication network" Internet "for federal state authorities and state authorities of the constituent entities of the Russian Federation" (Registered in the Ministry of Justice of the Russian Federation 04.09.2009 N 14705).] http://roskodeks.ru/news_full.php?nid=151250

PFSTEK-17. 2013. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17. [Requirements for the protection of non-state secret information contained in state information systems, approved by order of the Federal Service for Technical and Export Control dated February 11, 2013 N 17.] https://www.garant.ru/products/ipo/prime/doc/56603002/

Pigman, L. 2018. Reining In the Runet: The Kremlin's Struggle to Control Cyberspace. *Foreign Policy Research Institute.* https://www.fpri.org/article/2018/11/reining-in-the-runet-the-kremlins-struggle-to-control-cyberspace/

PMS-6. 2008. Приказ Министерства информационных технологий и связи РФ от 16 января 2008 г. N 6 "Об утверждении Требований к сетям электросвязи для проведения оперативно-разыскных мероприятий. Часть I. Общие требования". [Order of the Ministry of Information Technology and Communications of the Russian Federation dated January 16, 2008 N 6 "On approval of requirements for telecommunication networks for conducting operational search activities. Part I. General requirements".] http://base.garant.ru/192775/

Poore, S. 2003. What is the context? A reply to the Gray-Johnston debate on strategic culture. *Review of International Studies*, 29, 279-284. https://www.jstor.org/stable/20097850?seq=1#page_scan_tab_contents

PP-528. 2019. Постановление Правительства Российской Федерации от 30.04.2019 № 528 "Об утверждении Правил предоставления из федерального бюджета субсидии на создание и функционирование Центра мониторинга и управления сетью связи общего пользования, а также создание, эксплуатацию и развитие информационной системы мониторинга и управления сетью связи общего пользования". [Decree of the Government of the Russian Federation of April 30, 2019 No. 528 "On Approval of the Rules for Providing Subsidies from the Federal Budget for the Establishment and Operation of the Center for Monitoring and Managing a Public Communication Network, as well as the creation, operation and development of an information system for monitoring and managing a public communication network".] http://publication.pravo.gov.ru/Document/View/0001201905060004?index=0

PP-538. 2005. Постановление Правительства РФ от 27.08.2005 N 538 (ред. от 25.09.2018) "Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность". [Decree of the Government of the Russian Federation of August 27, 2005 N 538 (ed. September 25, 2018) "On Approval of the Rules for Interaction of Communication Operators with the Authorized State Bodies Conducting Operational-Investigation Activities".] http://www.consultant.ru/document/cons_doc_LAW_55326/

PP-758. 2014. Постановление Правительства Российской Федерации от 31 июля 2014 г. N 758 г. Москва "О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской

Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей". [Decree of the Government of the Russian Federation of July 31, 2014 N 758 Moscow "On Amendments to Certain Acts of the Government of the Russian Federation in Connection with the Adoption of the Federal Law" On Amendments to the Federal Law "On Information, Information Technologies and Information Protection" and separate legislative acts of the Russian Federation on streamlining the exchange of information using information and telecommunication networks".] https://rg.ru/2014/08/05/svyaz-site-dok.html

PP-1895. 2000. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895) (утратила силу). [The Doctrine of Information Security of the Russian Federation (approved by the President of the Russian Federation of September 9, 2000 N Pr-1895) (expired).] http://base.garant.ru/182535/#ixzz5pZXR2sMU

PPP-0101. 2017. Проект постановления Правительства РФ «Об утверждении показателей критериев значимости объектов КИИ РФ и их значений, а также порядка и сроков осуществления их категорирования». [Draft of the Decision of the Government of the Russian Federation "On the approval of indicators of the criteria for the significance of the objects of the CII RF and their meanings, as well as the procedure and deadlines for their categorization.] Проект 01/01/09-17/00073423

PUP-1. 2015. Draft of Information Security Doctrine of the Russian Federation. http://www.worldinwar.eu/information-security-doctrine-of-the-russian-federation-draft/

Putin, V. 2015. Meeting of the Valdai International Discussion Club. http://en.kremlin.ru/events/president/news/50548

Putin, V. 2016. Послание Президента Федеральному Собранию. [President's Speech to the Federal Assembly.] http://kremlin.ru/events/president/news/53379

Putin, V. 2018. Послание Президента Федеральному Собранию. [President's Speech to the Federal Assembly. http://kremlin.ru/events/president/news/56957

PZF 608767-7. 2018. проект федерального закона № 608767-7 "О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации" (в части обеспечения безопасного и устойчивого функционирования сети Интернет на территории Российской Федерации). [draft federal law No. 608767-7 "On Amendments to the Federal Law" On Communications "and the Federal Law" On Information, Information Technologies and Information Protection "(in terms of ensuring the safe and sustainable operation of the Internet in the Russian Federation).] http://www.lexfeed.ru/law/608767-7

Pynnöniemi, K. 2018. Russia's National Security Strategy: Analysis of Conceptual Evolution, *The Journal of Slavic Military Studies*, 31 (2), 240-256.

Raud, M. 2016. China and Cyber: Attitudes, Strategies, Organization. Tallinn: CCDCOE. https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf

Ramm, A., Kozatsenko, A & Stepovoi, B. 2019. Военный, красивый, суверенный: армия РФ создает закрытый интернет. Вся важная информация будет храниться только на серверах Минобороны. [Military, beautiful, sovereign: the army of the Russian Federation creates a closed Internet. All important information will be stored only on the servers of the Ministry of Defense.] https://iz.ru/854961/aleksei-ramm-aleksei-kozachenko-bogdan-stepovoi/voennyi-krasivyi-suverennyi-armiia-rf-sozdaet-zakrytyi-internet

RBA. 2013. Agreement between Belarus and the Russian Federation on cooperation in the field of international information security. http://www.pravo.by/main.aspx?guid=3871&p0=A01300055&p1=1

RCA. 2015. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 30 апреля 2015 г.][Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in the field of ensuring international information security dated April 30, 2015. http://static.government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf

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), 113-131. https://www.jinfowar.com/journal/volume-16-issue-4/should-%E2%80%98runet-2020%E2%80%99-be-taken-seriously-contradictory-views-about-cyber-security-between-russia-west

Rjabov, K. 2019. «Мультисервисная транспортная сеть связи» для Минобороны. Armeiskyj Vestnik. ["Multiservice Transport Communication Network" for the Ministry of Defense.] https://army-news.ru/2019/03/multiservisnaya-transportnaya-set-svyazi-dlya-minoborony/

Rogozin, D. 2013. Текст выступления Дмитрия Рогозина на пресс-конференции в "РГ". [Speech by Dmitry Rogozin at a press conference in the "RG".] https://rg.ru/2013/06/28/doklad.html

Rostekh. 2017. Ростех создал структуру для борьбы с киберугрозами. [Rostekh has created a framework for combating cyberthreats.] http://rostec.ru/news/4519332

Saaranen-Kauppinen, A. & Puusniekka, A. 2009. Menetelmäopetuksen tietovaranto. *Kvalitatiivisten menetelmien verkko-oppikirja.*

[Method Teaching Resource. Online Textbook for Qualitative Methods.] https://www.fsd.uta.fi/menetelmaopetus/kvali/index.html

Sanger, D & Perlroth, N. 2019. *U.S. Escalates Online Attacks on Russia's Power Grid*. New York Times. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?searchResultPosition=1

SBRF. 2011. Конвенция об обеспечении международной информационной безопасности (концепция). [Convention on ensuring international information security (concept).] http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

SBRF. 2012. "Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации" (утв. Президентом РФ 03.02.2012 N 803). [The main directions of the state policy in the field of ensuring the security of automated systems for managing production and technological processes of critical infrastructure facilities of the Russian Federation" (approved by the President of the Russian Federation on 03.02.2012 N 803).] http://www.consultant.ru/document/cons_doc_LAW_150730/

SBRF. 2013. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. [Basics of Russian Federation national policy on international information security to 2020.] http://base.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=178634&fld=134&dst=1000000001,0&rnd=0.5310172209117789

SBRF. 2014. Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом РФ 12.12.2014 N K 1274). [Extract from the Concept of the State System for Detection, Prevention and Elimination of the Consequences of Computer Attacks on Information Resources of the Russian Federation.] http://www.consultant.ru/document/cons_doc_LAW_181661/

SBRF. 2016. Draft of the information security doctrine of the Russian Federation. http://www.worldinwar.eu/information-security-doctrine-of-the-russian-federation-draft/

SCO. 2019. The Shanghai Cooperation Organisation (SCO). http://eng.sectsco.org/

Shactman, N. 2010. Wired: Insider doubt 2008 Pentagon hack was foreign spy attack (Updated). https://www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/

Siponen, M. & Baskerville, R. 2018. Intervention Effect Rates as a Path to Research

Relevance: Information Systems Security Example. *Journal of the Association for Information Systems*, 19 (4), 247-265. doi: 10.17705/1jais.00491

Shoigu, S. 2016. Расширенное заседание коллегии Министерства обороны. [Enlarged meeting of the board of the Ministry of Defense.] Speech at the College of Ministry of Defence, 22 December 2016. http://kremlin.ru/events/president/transcripts/53571

Skak, M. 2016. Russian strategic culture: the role of today's chekisty. *Contemporary Politics* , 22 (3), 324-341. http://www.tandfonline.com/doi/abs/10.1080/13569775.2016.1201317

Slugin, I. 2012. Регуляция сетевого пространства в России: текущая ситуация и возможные перспективы. [Regulation of network space in Russia: current situation and possible prospects.] *Бизнес, общество, власть*. 12. http://elibrary.ru/item.asp?id=22286947

Snyder, J. 1977. The Soviet Strategic Culture : Implications for Limited Nuclear Operations. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/reports/R2154.html.

Soldatov, A. & Borogan, I. 2015. *The Red Web*. New York: Public Affairs

Soldatov, A. 2017. The Taming of the Internet. *Russian Social Science Review*. 58 (1), 39-59.

von Solms, R. & van Niekerk, J. 2013. From information security to cyber security. *Computer and Security*, 38, 2013. https://ldc.usb.ve/~torrealba/sti-242/4ta_Clase/solms-2013.pdf

Stein, J. 2013. Threat Perception in International Relations. in Leonie Huddy, David O. Sears, and Jack S. Levy (eds) *The Oxford Handbook of Political Psychology* (2 ed.) DOI: 10.1093/oxfordhb/9780199760107.013.0012

TAdviser. 2016. Система оперативно-розыскных мероприятий. [The system of operational search activities.] http://www.tadviser.ru/index.php/Статья:СОРМ_(Система_оперативно-розыскных_мероприятий)

Tass. 2016. СМИ: в РФ разработали военный интернет для безопасного обмена секретной информацией. [In the Russian Federation developed the military Internet for the safe exchange of secret information.] https://tass.ru/armiya-i-opk/3715422

Tass. 2019a. Песков допустил гипотетическую возможность кибервойны против России со стороны США [Peskov allowed the hypothetical possibility of cyberwar against Russia by the US] https://tass.ru/politika/6557625

Tsernenko, E. & Demidov, O. 2015. Игра про правила. [Game by the book.] *Rossija v globalnoi politike*, 4. https://globalaffairs.ru/number/Igra-pro-pravila-17640

UNGA. 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. https://digitallibrary.un.org/record/786846

UNGA (2018a). Resolution Advancing Responsible State Behaviour in

Cyberspace in the Context of International Security. A/C.1/73/L.37. 18. October 2018. https://undocs.org/A/C.1/73/L.37

UNGA (2018b). Developments in the field of information and telecommunications in the context of international security. A/C.1/73/L.27/Rev.1. 29 October 2018. https://undocs.org/A/C.1/73/L.27/Rev.1

UP-9. 1992. Указ Президента РФ от 5 января 1992 г. № 9 «О создании Государственной технической комиссии при Президенте Российской Федерации». [Decree of the President of the Russian Federation of January 5, 1992 No. 9 "On the establishment of the State Technical Commission under the President of the Russian Federation".] https://www.lawmix.ru/pprf/98289

UP-24. 2000. Указ Президента РФ от 10.01.2000 N 24 "О Концепции национальной безопасности Российской Федерации". [Presidential Decree of January 10, 2000 N 24 "On the Concept of the National Security of the Russian Federation".] http://www.consultant.ru/document/cons_doc_LAW_25677/

UP-31. 2013. Указ Президента Российской Федерации от 15 января 2013 г. N 31с г. Москва "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации". [Decree of the President of the Russian Federation of January 15, 2013 N 31c Moscow "On the establishment of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation".] https://rg.ru/2013/01/18/komp-ataki-site-dok.html

UP-188. 1997. Указ Президента Российской Федерации от 06.03.97 № 188 «Об утверждении перечня сведений конфиденциального характера». [Presidential Decree of 06.03.97 № 188 “On Approving the List of Confidential Information”] http://dehack.ru/zak_akt/npa_prezidentarf/up188/

UP-203. 2017. Указ Президента Российской Федерации О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы. [Degree of –the- President of. the. Russian.Federation. on. the. Strategy.for.the Development of the.Information.Society.in the Russian Federation for 2017-2030.] http://www.kremlin.ru/acts/bank/41919

UP-314. 2004. Указ Президента Российской Федерации от 9 марта 2004 г. N 314 «О системе и структуре федеральных органов исполнительной власти». [Decree of the President of the Russian Federation of March 9, 2004 N 314 "On the system and structure of federal executive bodies”.] https://rg.ru/2004/03/11/federel-dok.html

UP-334. 1995. Указ Президента Российской Федерации от 03.04.1995 г. № 334 О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации. [Decree of the President of the Russian Federation of April 3, 1995 No. 334 On Measures for Compliance with the Legality in the Development, Production, Sales and Operation of Encryption Means, and the Provision of Services in the Field of Information Encryption.] http://clsz.fsb.ru/docs/gov/u334.htm

UP-569. 2017. Указ Президента Российской Федерации от 25.11.2017 г. № 569 О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085. [Decree of the President of the Russian Federation of November 25, 2017 No. 569 On Amendments to the Regulations on the Federal Service for Technical and Export Control, approved by Decree of the President of the Russian Federation of August 16, 2004 No. 1085.] http://kremlin.ru/acts/bank/42489

UP-620. 2017. Указ Президента Российской Федерации от 22.12.2017 г. № 620 О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. [Decree of the President of the Russian Federation of December 22, 2017 No. 620 On the improvement of the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation]. http://www.kremlin.ru/acts/bank/42623

UP-640. 2016. Указ Президента Российской Федерации от 30.11.2016 г. № 640 Об утверждении Концепции внешней политики Российской Федерации. [Decree of the President of the Russian Federation of 30.11.2016, № 640 On approval of the Concept of the foreign policy of the Russian Federation.] http://kremlin.ru/acts/bank/41451

UP-646. 2016. Указ Президента Российской Федерации от 05.12.2016 г. № 646 Об утверждении Доктрины информационной безопасности Российской Федерации. [Decree of the President of the Russian Federation of 05.12.2016, № 646 On approval of the Information Security Doctrine of the Russian Federation.] http://kremlin.ru/acts/bank/41460

UP-683. 2015. Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации". [Presidential Decree of December 31, 2015 N 683 "On the National Security Strategy of the Russian Federation.] http://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html

UP-1085. 2004. Указ Президента РФ от 16 августа 2004 г. N 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (с изменениями от 22 марта, 20 июля 2005 г., 30 ноября 2006.). [Decree of the President of the Russian Federation of August 16, 2004 N 1085 "Questions of the Federal Service for Technical and Export Control" (as amended on March 22, July 20, 2005, November 30, 2006.)] https://fstec.ru/component/attachments/download/234

Vendil Pallin, C. & Franke, U. 2012. Russian Politics and the Internet. *FOI report.* https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--3590--SE

Vendil Pallin, C. 2016. Internet control through ownership: the case of Russia, *Post-Soviet Affairs*, DOI: 10.1080/1060586X.2015.1121712

Vendil Pallin, C. 2019. *Russian Information Security and Warfare Strategy*. Chapter 17 in R Kanet (ed.) *The Routledge Handbook of Russian Security*. Routledge.

Voejkov, Denis. 2017. Сверхсекретная ГИС ФСБ начала выходить из тени. [The top secret GIS of the FSB began to come out of the shadow.] *CNews.* .http://www.cnews.ru/news/top/2017-10-06_sverhsekretnaya_gis_fsb_nachala_vyhodit_iz_teni

Wirtz, J. 2015. Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. Tallinn: CCDCOE. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf

Yarovaya M. 2013. Игорь Ашманов: "Сегодня информационное доминирование – это все равно, что господство в воздухе". [Igor Ashmanov: "Today information domination is the same as air superiority] https://ain.ua/2013/05/01/igor-ashmanov-segodnya-informacionnoe-dominirovanie-eto-vse-ravno-chto-gospodstvo-v-vozduxe

YA. 2009. Yekaterinburg agreement https://ccdcoe.org/sites/default/ files/documents/SCO-090616-IISAgreementRussian.pdf - linkki ei toimi 1.6.2019

Yefremov, A. 2017. Formation of the concept of information sovereignty of the state. https://www.researchgate.net/publication/315671432_Formirovanie_koncepcii_informacionnogo_suvereniteta_gosudarstva

Zaman, R. 2009. Strategic Culture: A "Cultural" Understanding of War. *Comparative Strategy*, 28 (1), 68-88, DOI: 10.1080/01495930802679785

Zhuang, J. & Hu F. 2014. Game-Theoretic Analysis of Attack and Defense in Cyber-Physical Network Infrastructures. https://www.eng.buffalo.edu/~jzhuang/Papers/HZR_ISERC2012.pdf

ORIGINAL PAPERS

I

RUSSIA: A CYBER FORTRESS BESIEGED

by

Kari, Martti J. & Kuusisto, R. (2017)

ECCWS 2017: Proceedings of the 16th European Conference on Cyber Warfare and Security (Dublin, 2017), pp. 593–601

Reproduced with kind permission by ECCWS 2017.

Russia: A Cyber Fortress Besieged

PhD student Martti J Kari, Adjunct Professor Rauno Kuusisto
Faculty of Information Technology, Jyvaskyla University, Finland
majokari@student.jyu.fi
Rauno.k.kuusisto@jyu.fi

1. Abstract

A limited amount of information has been published about Russian cyber threat scenarios. However, there is enough information scattered in official Russian documents to build up at least a satisfactory description of the Russian perception of cyber threats and the targets of that threat. Our paper discusses the Russian perception of cyber threats and the targets of the cyber threats publicly described by the Russians. As source material, we used official Russian documents such as strategies, doctrines, laws and presidential decrees. The material includes twelve laws of the Russian Federation and nine presidential decrees. In addition, the materials include four information security agreements, seven Russian Security Council documents, and doctrine and guidance documents from various ministries.

To address our topic we have applied grounded theory. Grounded theory is well suited to studying Russian cyber threats and targets because very little theoretical and structured information has, to date, been published about the subject. The Russian cyber threat assessment reflects the tension in the international situation. One of the axioms of Russian history is, according President Vladimir Putin, that the Soviet Union has been a besieged fortress. It is surrounded by potential enemies and under constant threat of attack from the West. For modern Russia, after the annexation of Crimea and the wars in eastern Ukraine and Syria, war has become a justification for the Kremlin's image of Russia as once again surrounded by enemies and under threat of attack. These events make it seem that Russia continues to view itself as a fortress besieged, so we extend this perception to the cyber realm. Our hypothesis is that the Russian cyber threat assessment is based on the fortress besieged model, similar to the one that exists in other Russian threat scenarios. In the study, a key concept that emerged is that of the cyber target. This concept, along with the individual objects facing cyber threats, have shaped the country's strategic national interests, including information, information infrastructure, the Russian Armed Forces and other targets such as the energy sector, banking and industry.

Keywords: Russia, cyber threat, cyberspace, cyber operation, critical information infrastructure, information resources

2. Introduction

The purpose of computer science and information systems as a discipline and a branch of study is to understand information systems from the perspective of information security management and in particular from the threat perspective. In this paper, we examine Russian information systems and describe the Russian perception of the cyber threat to Russia based on official documents. Our hypothesis is that that the Russian cyber threat assessment includes the fortress besieged model, similar to what exists in other Russian threat scenarios (Kolesnikov 2016).

The information security doctrine of the Russian Federation (UP-646 2016) defines the threat to information security as a complex of actions and factors, creating danger for Russian national interests in information space. Information space is a complex of information, objects of informatization, information systems, websites, communication networks and information technologies. Informatization means social, economic and technical processes to adopt and expand information technology in society and throughout the country as well as to secure access to information resources. Information space includes subjects creating, generating and processing information, subjects developing or using information technology or managing information security. It also includes mechanisms regulating the information relations in society.

Information warfare can be information technical, when informational technical systems are objects of influence in cyber space or information psychological, when the adversary tries to influence a person's mind, his or her moral and mental world, social political opinions and ability to make decisions (Kamyshev 2009). Cyber space is a sphere of activity in the information space. Cyber space consists of technological infrastructure, which enables the internet and the functionality of other telecommunication channels of telecommunication networks, and all the human activity that occurs on the internet and via other communication channels. Cyber space is a limited area of information space (SBRF 2013). In this paper, *cyber threat* refers to cyber attacks, cyber intelligence, and other activities in cyber space or through cyber space, which either cause a threat to Russia or create the feeling of danger or real danger.

Terrorism and war have become normal phenomena in everyday Russian life. After the annexation of Crimea and the wars in eastern Ukraine and Syria, war has become routine and now serves as one justification for the Kremlin's image of Russia as "a besieged fortress" surrounded by enemies and under the threat of attack (Kolesnikov 2016). In the Russian military doctrine from 2010 and 2014, the deployment of NATO forces near Russia's borders and the organization's expansion are mentioned as military dangers. The deployment of antimissile defence systems in Europe is also considered a danger (MDRF 2010, 2014). This perception of being surrounded by adversaries justifies the fighting of wars, large defence spending and antiterrorist legislation, and gives the Kremlin the opportunity to name external as well as internal enemies.

The 2014 doctrine states that the threats are extending to information space as well as within Russia. In the 2014 doctrine, a new danger is the use of information and communication technology to achieve military political goals (MDRF 2014). In his summary of 2016, minister of defence Sergei Shoigu (2016) said that challenges to Russia's security are increasing. NATO will locate units in Eastern Europe, and NATO intelligence is active within Russia's borders. American antimissile systems in Europe are in initial operational readiness and more will be delivered to Japan and South Korea. Shoigu draws a picture of Russia as besieged by the USA and its allies in Europe as well as in Asia. These threats create the perception within Russia that the country is a fortress besieged. This perception becomes, in the spirit of grounded theory, a basis for using the fortress besieged view as a theoretical phenomenon. Therefore, we construct our analysis based on that presupposition and study if the available research material supports this hypothesis. The theory of Russia's perception of being a fortress besieged leads us to formulate the research problem as follows:

- Does the Russian cyber threat assessment correlate with the Russian general threat assessment?
- Who is causing the cyber threat to Russia, by which means and what are the targets of that threat?

In this paper we follow the hermeneutical science tradition, which influences how we apply grounded theory. In our approach, we set the hypothetical end-state abstraction level at the beginning of our research. During the research process, we collect and analyse information to increase our understanding about the reachability of that abstraction and adjust the whole process to reach the relevant end-state. If the hypothetical end-state statement proves to be non-valid, the process will reveal that as well.

3. Methodology

3.1 Method: grounded theory

In our research we have applied grounded theory because it is well suited for studying topics about which there is little published theoretical and structured information. For our study we adopted the version of grounded theory developed by Anselm Strauss and Juliet Corbin (1990). Compared with the original version of grounded theory, the Strauss-Corbin version is more structured. The Strauss-Corbin version accepts that the researcher is already familiar with the theoretical literature related to the studied subject. In contrast to Glaser's improvisation- and intuition-orientated version, where the researcher should avoid the theoretical subject-related literature at the beginning of his study to prevent the formation of unconscious bias about the research subject, in the Corbin-Strauss version the research problem is defined deductively in advance.

At the beginning of data collection, we also started the coding process. In the first phase, consisting of open coding, we read the data carefully line by line. The aim was to find, identify, name and describe the concepts and categories related to cyber security. We conceptualized the phenomena in the data related to the cyber threat to Russia. At the same time, we started to group the concepts into categories.

A concept is an idea, an image and a mental picture, which describes the phenomenon or its distinctive characteristics in a generic way. The examples of the concepts found in the data are the critical object of the information infrastructure, information in databases, access to information, and cryptologic keys. The concepts are used to group the collected data into categories. A category is a group of similar concepts, and categories are used to generate a theory. The categories of cyber threat which emerged from the data are the target of the cyber threat, the cause, the source or the factor of the cyber threat, the method or the means, and the consequences of the cyber threat.

In the axial coding, we established the connections between the concepts and categories and defined the core category. The core category is a category which frequently occurs in the data and is logical, coherent and consistent with the rest of the data (Strauss and Corbin 1994). The core category of our study is the target of the cyber threat. During this period, we continued data collection, with the coding process guiding the theoretical sampling until saturation. After the saturation point, the theoretical sampling no longer brought more information related to the research questions.

The theory building was initiated during the selective coding. In grounded theory, *theory* refers to a collection of interrelated, well-defined and well-developed concepts that form an integrated frame of reference, which can in turn help to explain or predict the phenomena being studied. In the theory creation phase, we grouped the concept data in a new way, with subcategories formed in between the concepts and the category. For example, the concepts *database* and *telecommunication network* were part of the subcategory *information infrastructure*, which belongs to the category *target of the cyber threat*. The other subcategories of the targets of the cyber threat are *strategic interests*, *information*, *armed forces*, and *other targets*.

To maintain the linkage between the categories, we created tables from the subcategories, and the tables were given the titles *strategic interests*, *information infrastructure*, *information, Armed Forces*, and *other targets*. The columns of the tables were formed from the categories, that is to say the target, the cause and the method of the cyber threat.

We coded the data and compiled the tables twice to verify that the tabular format was a logical and practical way of building the theory as well as that the concepts and the categories in the tables are accurate. Another reason to recode the data is that after the first tabulation, new cyber security documentation was published in Russia. In July 2016, Russian parliament approved the so-called Yarovaya laws, amendments to the law on combating terrorism as well as to the Criminal Code (374-FZ 2016, 375-FZ 2016). In addition, a new Russian information doctrine was published in December 2016 (UP-646 2016).

3.2 The structure of the material

We studied and coded 55 official Russian documents related to cyber security. The documents studied cover the years 1993 to 2016. From these documents, the study data included three international cyber security agreements, 11 Russian Federation (RF) laws, six presidential decrees and five Security Council documents and three Ministry of Defence documents. Even though most of the sources are webpages, they can be considered as valuable sources because they are published by state Russian authorities as legislative and doctrine documents.

According the law on strategic planning (172-FZ 2014) the hierarchy of documents for strategic planning is

- Annual speech of the president to the Federal Assembly
- Strategy for the socioeconomic development of Russia
- National security strategy
- Main directions and bases of politics
- Doctrine documents
- Other records and documents

The Russian Federation President's annual state-of-the-nation address to the Federal Assembly is the guideline for strategic planning in Russia (FZ-172 2014). In his annual speech in December 2016, President Vladimir Putin (2016) mentioned that because of the risks included in digital technologies Russia had to strengthen its defences against cyber threats and make all the elements of its infrastructure, financial system, and state leadership and management more stable.

From the legal point of view, the documents dealing with cyber security are laws, decrees and other legislative documents and normative and methodological documents (Lapina, Revin and Lapin 2004, Komarov 2016).

In the following section, we introduce the results of our analysis. We also present a possible structure for the threat experienced by Russia that leads to the fortress-besieged pattern of thinking.

4. Analysis results

In the Russian definition, information warfare is a struggle between two or more states in the information space (MORF, 2011). The goals of information warfare are to

- cause harm to information systems, processes, resources and other critically important objects
- revolutionize political, economic and social systems and organizations
- destabilize state and society by psychological processing
- constrain a state to make decisions that are favourable to its adversary

The coding of the concepts of the cyber threat targets created groups of concepts, which were formed into five subcategories. The first subcategory of cyber threat targets is Russia's strategic interests. One part of these strategic interests are Russian national interests – such as sovereignty, territorial integrity and constitutional order – which can be threatened in or through cyber space by terrorists or criminals (UP-24 2000, MDRF 2010, MDRF 2014, UP-683 2015, SBRF 2016). The production and use of cyber weapons threaten Russia's national interests (JA, 2009; RBA, 2013; SBRF, 2013a). In addition, abuse of dominance by some unnamed states in cyber space is a threat to Russia. Western intelligence services and terrorist organizations can violate Russia's sovereignty or territorial integrity through cyber intelligence or cyber attacks (UP-24 2000, UP-683 2015). The technical intelligence for Russian state organs as well as its defence industry has been increased (UP-646 2016).

Russia's national interests in cyber space are another part of Russian strategic interests as the targets of cyber threats (SBRF 2000, SBRF 2011, SBRF 2016). Russian citizens have a constitutional right to have access to information as well as a right to the integrity of their privacy while using information technology (UP-646 2016). The stable and safe functioning and independence of the Russian segment of the internet, RUNET, is one of its strategic interests. Yet because the internet is governed by ICANN, actors outside of Russia can, according to Russia, block access to the internet and destabilize the functioning of RUNET (SBRF 2012). One threat to Russia's strategic interests is preparations by Western countries for an information war and aspirations to change information space into a war zone (MDRF 2010, MDRF 2014). This could lead to a cyber arms race. Russia's technological backwardness in software and hardware production has created a dependence on foreign information technology. This underdevelopment weakens Russia's cyber defences, facilitates cyber intelligence operations in Russia and gives Western special services an opportunity to influence Russia's information resources (UP-683 2015, SBRF 2016, UP-646 2016). Table 1 presents Russian strategic interests as targets of cyber threats.

Table 1. Russian strategic interests as targets of cyber threats

Originator or cause of threat	Target of cyber Threat	Method or means of cyber threat
USA, Western countries, Nato Western special services Terrorists Extremist movements	Russia's national interests Sovereignty Territorial integrity Political stability, independence and constitutional order	Cyber terrorism, Cyber crime Production and use of information weapons Dominance of state in cyber space Cyber intelligence, Cyber attack
Developed foreign states and political and economic actors Terrorists Criminals Intelligence and special services Extreme movements	National interests in information space Constitutional rights of citizens to access information and to the integrity of their privacy while using information technology	Development of information technology and methods in a way that is disadvantageous to Russia Use of information technology to achieve geopolitical goals Cyber intelligence, Cyber attack
Western countries, Nato	Changing the information space into a war zone	The spread of confrontation into information space Aspiration of states to dominance in information space Preparations for information war
Use of dominant position of leading states in cyber space Dependence of Russia on foreign information technology Monopolization of information technology production	Technological backwardness in software and hardware including a lack of supercomputers Information technology production	Monopoly of software production Exploitation of dominant position in information space
Natural phenomena Terrorists Extremist movements	Critically important objects of Russian Federation infrastructure	Cyber attack Cyber malfunction
Terrorist organizations Information terrorism Information crime	Automated information systems of state management and decision-making systems	Use of information weapons
Actors outside of Russia Internet governance by the USA	Functioning and independence of the Russian segment of the internet	ICANN

Information resources is the second subcategory of the targets of the cyber threat experienced by Russia. Information resources include secret and confidential information (40-FZ 1995, 61-FZ 1996), state secrets (4524-FZ 1993, 5485-FZ 1993, 40-FZ 1995, 61-FZ 1996, SBRF 2000, UP-646 2016), business and service secrets (UP-188 1997, 149-FZ 2006), personal and family secrets (152-FZ 2006, SBRF 2016), information necessary for society, open information resources and personal data. Developed foreign states (SBRF 2000), terrorist organizations and cyber criminals (JA 2009, SBRF 2013b, RBA 2013, RCA 2015) are violating the confidentiality, integrity and availability of Russian information resources. Unauthorized intrusions into information systems to steal, manipulate, forge, change or destroy information or to block access to information are seen as cyber threats to Russia. Cyber attacks can be directed at the information saved in databases, processed in computers or transmitted in telecommunication networks (SBRF 2000, UP-24 2000, JA 2009, RBA 2013, RCA, 2015). In addition, saving, processing and transmitting the information against regulations, technical malfunctions and malware defects are mentioned as cyber threats (SBRF 2011). The information resources of the Russian Federation as the targets of cyber threats are presented in Table 2.

Table 2. Information resources of the Russian Federation as targets of cyber threats

Originator or cause of threat	Target of cyber threat	Method or means of cyber threat
Information terrorism Cyber crime Private persons	Information resources of the Russian Federation Integrity of information	Intrusion into information systems Malware, DDoS attack, Cyber attack Technical intelligence

	Availability of information Confidentiality of information	Unauthorized remote control of system
Information crime Developed foreign states Private persons	Secret and confidential information Very important, top secret, secret information Handling, saving and transmitting of state secrets Business secrets, service secrets	Intrusion into information systems Cyber attack, Cyber intelligence Handling and transmitting information against regulations Technical malfunctions, malware defects
Cyber crime	Information necessary for society Databases, including those with personal data Personal and family secrets Personal data	Intrusion into information systems Limitation of access to information Manipulation of information Unauthorized use of information Technical intelligence Malware, DDoS attack
Information crime Information terrorism Developed foreign states	Open information resources including archives Information in transmission path Integrity of information Availability of information Confidentiality of information	Limitation of access to information Manipulation of information Unauthorized collection and use of information Cyber attack, Cyber intelligence Intrusion into information recourses

Information infrastructure is the third subcategory of the targets of the cyber threat. The information infrastructure includes Russia's critical information infrastructure, its components and functions, information telecommunication networks and their automated control systems, special communication networks, tele operators, and information processing and information security management technology. The information processing and information security management technology includes software, hardware, operating systems, encryption keys and cryptographic protection systems. A cyber threat to the Russian information infrastructure can be caused by foreign states, cyber terrorists and criminals, extreme movements and harmful natural phenomena (40-FZ 1995, UP-334 1995, 5-FZ 1996, UP-24 2000, 152-FZ 2006, MORF 2011, 1-FZ 2013, UP-31 2013, SBRF 2012, SBRF 2013a, SBRF 2013b, RBA 2013, RCA 2015, SBRF 2016, UP-646 2016). The information infrastructure of the Russian Federation as a target of cyber threats is presented in the Table 3.

Table 3. Information infrastructure of the Russian Federation as a target of cyber threats

Originator of threat	Target of cyber threat	Method or means of cyber threat
Unequal division of internet resources	Stable and safe functioning of the internet	
Foreign states Information terrorism Cyber crime Harmful natural phenomena	Information infrastructure, its objects and stable functions Tele operators	Development and use of information weapons Preparations for information war Threats caused by nature and technology Malware Cyber attack, Cyber intelligence Capability for cyber attacks
Foreign states Terrorists Terrorist organizations Extremist movements	Russia's critical information infrastructure, its components and functions Information telecommunication networks and their automated control systems and their functioning Special communication networks	Information technical influence Malware Breach of information security Cyber attack, Cyber intelligence Cyber malfunction Disturbance of information and telecommunication systems Monopoly of software production Exploitation of dominant position in information space
	Information processing technology	Technological damage

	Information systems Software, operating systems Database programs Information in computers Cryptographic protection of information in automated information processing and transmitting systems Encryption keys	Viruses, malware Internet attack Illegal intrusion into information systems Disturbing the functioning of information systems
	Automated control systems Automated control system of critically important objects	Unauthorized intrusion into information systems Cyber attack Cyber malfunction Maintenance activity by foreign companies Remote use and control by foreign companies

The Armed Forces of the Russian Federation is the fourth subcategory. The information and communication infrastructure as well as the information resources of the Armed Forces are seen as targets of cyber threats (JA 2009, SBRF 2000, MDRF 2010, SBRF 2012, RBA 2013, MDRF 2014). Foreign special services, terrorist organizations and extremist movements are targeting the information and communication infrastructure and information resources of the Russian Armed Forces in cyber space (61- FZ 1996, SBRF 2000, MDRF 2010, MDRF 2014). Russia considers strategic missile warning and defence systems, air and space defence forces and strategic missile forces the main targets of possible cyber espionage and cyber attacks. The attacker tries to lower the defence capability of these strategically important systems and forces (JA 2009, MDRF 2010, SBRF 2012, SBRF 2013b, RBA 2013, MDRF 2014).

During a pre-war period and in the first phase of any hostilities, the mobilization of the Russian Armed Forces (i.e. the build-up of wartime troops) and strategic deployments (the deployment of wartime troops to operational areas) would be targets of cyber attacks. In addition, the logistic systems supporting mobilization and strategic deployment are seen as the targets of cyber attacks before the outbreak of a war. The readiness of the Armed Forces is also targeted by foreign intelligence services in peacetime (61-FZ 1996, JA 2009, MDRF 2010, SBRF 2012, MDRF 2014). The Armed Forces of the Russian Federation as targets of cyber threats are presented in Table 4.

Table 4. The Armed Forces of the Russian Federation as targets of cyber threats

Originator of threat	Target of cyber threat	Method or means of cyber threat
Terrorist organizations Extremist movements	Combined information and communication infrastructure of the Russian Armed Forces and branches	Intrusion into information networks Cyber intelligence, Cyber attack
	Information resources of the Armed Forces Software, Computers	Information weapons
	Command and control system	
	Missile warning and defence systems	Information weapons
	Air and space defence	Information weapons
	Activity of strategic missile forces	
	Mobilization and strategic deployment	
	Readiness of the Armed Forces	
	Logistic infrastructure	
	Automated command and control systems of troops and weapons	

The last subcategory includes targets other than those mentioned above. Electrical grids and the functioning of nuclear power plants are targets of cyber attacks (MDRF 2010, SBRF 2012, MDRF 2014, RCA 2015, SBRF 2016, UP-646 2016). The most targeted industry sectors are the defence, chemical and medical industries, probably due to their strategic importance for the defence of Russia. There are a number of typical threat scenarios: terrorists launch a cyber attack on the automated control systems of industrial processes (SBRF 2012, MDRF 2014, RCA 2015), cyber criminals attempt to intrude into databases and the control systems of the banking sector, or cyber criminals target the Russian stock market, taxation and customs systems (UP-334 1995, SBRF 2000, 152-FZ 2006, RBA 2013, RCA 2015, SBRF 2016). The other targets of cyber threats are presented in Table 5.

Table 5. Other targets of cyber threats

Originator of threat	Target of cyber threat	Method or means of cyber threat
Terrorist organizations	Electrical grids	Cyber attack
Terrorist organizations	Functioning of nuclear power plants	
	Information resources of the defence industry	Cyber intelligence
	Automated control systems of defence industry processes	Cyber attack
	State organs	Cyber intelligence
	Scientific organizations	Cyber intelligence
	Material and raw material supply	
Terrorist organizations Extremist movements	Production facilities Management of production structure	
Terrorist organizations	Logistics infrastructure	Cyber attack
	Chemical industry: automated process control systems	Cyber attack
	Medical industry	

5. Conclusions

The cyber threats to Russia are increasing and becoming more diverse. On a strategic level, these threats are part of the wider threat to Russia's strategic interests. Information and the information infrastructure are targets of both external and internal cyber threats. In the data the principle of information security management data is mentioned as balancing between citizens' need for the free exchange of information and the limitations caused by the needs for national security in the information domain. Another principle is to have a sufficient amount of resources for information security management and for the continuous monitoring of information security threats. These principles probably indicate the increasing control of the Russian segment of internet by the security authorities as part of the response to internal and external threats in the information space.

As one part of strengthening the defence of the Russian cyber fortress, the data revealed a lack of supercomputers as well as a need for the domestic production of hardware and software. The previous doctrine from 2000 names the underdevelopment and backwardness of Russian information technology as a threat to the country's information security. Over the past decade, Russia has not managed to reduce the lead of Western countries in this area. The insufficient level of development of domestic information technology, services and production capabilities generate dependence on foreign information technology. This causes Russia's social and economic development to become dependent on the geopolitical interests of foreign countries.

One way mentioned in the data to mitigate the threat caused by the superiority of the Western countries in the information sphere is Russia's aspiration to create international legal norms, which would prevent the use of information technology for military purposes not in compliance with international law and for terrorist, extremist or criminal purposes. Cyber attacks and cyber espionage against Russia have intensified, which requires better management of information security by Russian authorities. The main opportunities to improve information security are increasing the monitoring of RUNET, creating international legal norms to prevent uses of internet that are harmful to Russia, and the development of Russia's own information technology industry, including research and development activity.

In the Russian cyber threat assessment, a similar fortress besieged model is seen as in other threat assessments. Russia's leadership feels that Russia is surrounded and threatened by hostile states and non-state actors in cyber space as well. The creators of the cyber threat are Western intelligence and special services along with terrorists and extremist movements. Different branches of the Russian administration and different ministries and agencies emphasize different issues in their cyber threat assessments, but the basic structure of the targets and the threat is common.

In this study, we focused on the Russian perception of the targets, originators and methods of cyber threats. In future research, we will examine how Russia's response to these cyber threats is described in the Russian official documents.

6. ACKNOWLDGEMENTS

We are grateful to Katri Pynnöniemi, Senior Research Fellow at the Finnish Institute of International Affairs, and Pauliina Hirvonen, PhD student at the University of Jyväskylä, who both gave helpful suggestions and guidance.

REFERENCES

Corbin, J. & Strauss, A. (1990) "Grounded Theory Research: Procedures, Canons, and Evaluative Criteria", *Qualitative Sociology*, Vol 13. No 1, pp 3-21.

JA (2009) Yekaterinburg agreement, 16 July 2009, [online], https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf

Kamyshev, E. (2009) *Информационная безопасность и защита информации.* Federalnoe Agenstvo RF po nauke i obrazovaniju. Tomsk.

Kolesnikov, A. (2016) "Do Russians Want War?" [online], http://carnegie.ru/2016/06/14/do-russians-want-war-pub-63743

Komarov, A. (2016) Нормативные документы по безопасности АСУ ТП, АСУ ПиТП, КСИИ, КВО, КИИ, [online], http://www.securitylab.ru/blog/personal/zlonov/144489.php

Lapina, M., Revin, A. & Lapin, V. *Informatsionnoe Pravo*. M. Juniti-dana. Zakon i pravo.

MDRF (2010). Military doctrine of the Russian Federation, [online], http://rg.ru/2010/02/10/doktrina-dok.html

MDRF (2014) Military doctrine of the Russian Federation, [online], http://www.scrf.gov.ru/documents/18/129.html

MORF (2011) The conceptual view of activity of the Armed Forces of the Russian Federation in information space, [online], http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle

Putin, V. (2016) Speech at the College of Ministry of Defense, 1 December 2016, [online], http://kremlin.ru/events/president/news/53379

RBA (2013) Agreement between Belarus and the Russian Federation on cooperation in the field of international information security, 25 December 2013, [Online], http://www.pravo.by/main.aspx?guid=3871&p0=A01300055&p1=1

RCA (2015) Agreement between the Russian Federation and China on cooperation in the field of international information security, 8 May 2015, [Online], http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf

SBRF (2000) Information security doctrine of the Russian Federation, [online], **http://www.scrf.gov.ru/documents/5.html**

SBRF (2011) Convention on ensuring international information security (Draft), [online], http://www.scrf.gov.ru/documents/6/112.html

SBRF (2012) Main directions of state policy on the security of automated production and process control systems of critical infrastructure in the RF, [online], http://www.consultant.ru/document/cons_doc_LAW_150730/

SBRF (2013) Basics of Russian Federation national policy on international information security to 2020, [online], http://base.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=178634&fld=134&dst=1000000001,0&rnd=0.5310172209117789

SBRF (2016) Draft of the information security doctrine of the Russian Federation, [online], http://www.scrf.gov.ru/documents/6/135.html

Shoigu, S. (2016) Speech at the College of Ministry of Defence, 22 December 2016, [online], http://kremlin.ru/events/president/transcripts/53571

Strauss, A. & Corbin, J. (1994) Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory, 2nd ed., SAGE, Thousand Oaks, CA, USA.

UP-24 (2000) Decree of the president on the concept of national security of the Russian Federation, [online], http://www.consultant.ru/document/cons_doc_LAW_25677/

UP-31 (2013) Decree of the president on a monitoring system for cyber attack on the Russian Federation, [online], https://rg.ru/2013/01/18/komp-ataki-site-dok.html

UP-188 (1997) Decree of the president on approving the list of confidential information, [online], http://dehack.ru/zak_akt/npa_prezidentarf/up188/

UP-334 (1995) Decree of the president on the production and use of cryptographical devices, [online], http://clsz.fsb.ru/docs/gov/u334.htm

UP-646 (2016) Decree of the president on the approval of the Information Security Doctrine of the Russian Federation, [online], https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

UP-683 (2015) Decree of the president on the national security strategy of the Russian Federation, [online], http://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html

1-FZ (2013) Proposal for the federal law on the security of critical information infrastructure, [online], http://rg.ru/pril/article/83/27/52/zakonoproekt.doc

5-FZ (1996) Federal law on foreign intelligence [online] http://svr.gov.ru/svr_today/doc02.htm

40-FZ (1995) Federal law on the Security Service of the Russian Federation, [online], http://docs.cntd.ru/document/9011123

61-F (1996) Federal law on defence [online] http://rg.ru/1996/06/06/oborona-dok.html

149-FZ (2006) Federal law on information, technology and information protection, [online] http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108264

152-FZ (2006) Federal law on personal information, [online], http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108261

172-FZ (2014) Federal law on strategic planning of the Russian Federation, [online], http://base.garant.ru/70684666/

374-FZ (2016) Amendments to Federal Law on combating terrorism" [online] http://pravo.gov.ru/laws/acts/54/5155524510601047.html

375-FZ (2016) Amendments to the Criminal Code of the Russian Federation and the Criminal Procedure Code, [online], http://publication.pravo.gov.ru/Document/View/0001201607070042

4524-1-FZ (1993) Federal law on organs of governmental communication and information, [online,] http://zakonbase.ru/content/part/138824

5485-FZ (1993) Federal law on state secrets, 21 July 1993, [online] http://www.consultant.ru/document/cons_doc_LAW_2481/

II

THE CONCEPT OF THE CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

by

Kari, M. (2018).

ICCWS 2018: Proceedings of the 13th Internation-al Conference on Cyber Warfare and Security (Washington, DC, 2018), pp. 543–551

Reproduced with kind permission by ICCWS 2018.

The Concept of the Critical Information Infrastructure of the Russian Federation

PhD student, Colonel (retired) Martti J. Kari
University of Jyväskylä
Jyväskylä, Finland
majokari@student.jyu.fi

Abstract: In December 2016, President Vladimir Putin signed the Information Security Doctrine of the Russian Federation (RF), which defines one of the national interests of the RF in the information sphere to be ensuring sustainable and uninterrupted functioning of its critical information infrastructure (CII). The doctrine, however, fails to define the concept of CII. This paper describes the development of the concept of the critical information infrastructure of the Russian Federation (CIIRF) starting from the year 2000 when the RF published its first doctrine regarding information. The concept of the CIIRF is important to define because it helps to understand the threats Russia perceives in the information sphere, and it serves as one of the basic terms in research on Russian information security management. Though a number of studies have been published about CII in the West or about CII in general, there has been relatively little about the CIIRF.

The research method is grounded theory, which is appropriate because there is a lack of theoretical and structured information about the subject. The study is based on official Russian documents related to information security. These include the Russian Federation's information security doctrines, draft legislation and laws as well as documents from the RF Security Council and Ministry of Defence.

The concept of the CIIRF has been in development since 2000. The deterioration of the relationship between Russia and the West can be seen in how the concept has become increasingly security and defense oriented. CII Policy Directions 2012 contained the first official definition of the CIIRF. The document defines the CIIRF as a complex of automated systems for managing critically important objects (CIOs) and for enabling their connections with information networks. These systems are subsequently used for state management, ensuring defense capability, and maintaining security as well as law and order. Any violation of these may have severe consequences. In the CII Security Law 2017, the importance of the strategic industries well as of the energy sector has also clearly risen.

Keywords: Russian Federation, critical information infrastructure, critically important object

1. Introduction

On December 5, 2016, Vladimir Putin, the President of the Russian Federation, signed a new Information Security Doctrine, replacing the Information Security Doctrine published in 2000. The new Information Security Doctrine (UP-646, 2016) defines the threat to information security as a complex of actions and factors that represent a danger to Russian national interests in information space.

In the Russian definition, *information space* is a complex of information, objects of informatization, information systems, websites, communication networks, and information technologies. Informatization means social, economic, and technical processes for adopting and expanding information technology throughout society and securing access to information resources. Information space includes creating, generating, and processing information, developing, and using information technology or managing information security. It also includes mechanisms regulating the information relations within society (UP-646, 2016).

According to the Information Security Doctrine 2016, one of the national interests of the RF in the information sphere is ensuring sustainable and uninterrupted functioning of the information infrastructure and especially the functioning of the CIIRF and the Russian portion of the Internet during peacetime, periods of aggression, and wartime. The CIIRF is not defined in the Information Security Doctrine, nor is there a list of the components, in Russian terms, of the objects of the CIIRF (UP-646, 2016).

As a discipline, computer science and information systems tries to understand and explain information systems. In this article, my aim is to understand and examine the concept of the CIIRF. I outline the development of the Russian concept of the CIIRF over the last two decades. Even though there is a terminological and conceptual resemblance between Russia's critical information infrastructure and the same term used in the United States and the European Union, it is important to define and understand the meaning and content of the Russian interpretation of CII.

The term helps to understand Russian threat perceptions in information space, and it serves as one of the basic terms in the research on Russian information security management. At the beginning of this study, I briefly describe two Russian terms: *information infrastructure* and *critical infrastructure*. After that, I examine the evaluation of the Russian term CIIRF using definitions found in Russian official documentation since the publication of the Information Security Doctrine in 2000.

2. Information Infrastructure and Critical Infrastructure

The information infrastructure of the RF is defined in the 2015 Russia–China Cyber Security Pact (RCPact, 2015) and in the 2016 Information Security Doctrine (UP-646, 2016). The information infrastructure of the RF is a complex of objects of informatization, information systems, websites, and communication networks in RF territory or in territories under RF jurisdiction or used based on international treaties of the RF (UP-646, 2016). The information infrastructure is a part of Russia´s information resources. Another part of these resources is the information itself and how it flows (MORF, 2011; SBRF, 2011; RBRPact, 2013; RCPact, 2015).

Information refers to all kinds of information (e.g., messages, data) regardless of its form. Information can be divided into public information and classified information (FZ-149, 2006). An information system is a complex of information contained in databases and information technologies as well as the technical means used for the processing of information (FZ-149, 2006; SBRF, 2011).

When the function of a *critical important object* is violated or terminated, it can lead to a loss of economic management of the state, of a constituent entity of the state or its administrative-territorial unit, or result in a significant reduction in the safety of the population (RBRPact, 2013). Critical important structures are objects, systems and institutions of the state that may have consequences for national security, including the security of the individual, society and the state (Yekaterinburg A, 2009).

3. Critical Information Infrastructure of the RF

3.1 Information Security Doctrine 2000

The development of critical information infrastructure as a term and concept began in 2000 when the IS Doctrine of the RF (SBRF, 2000), hereinafter ISD 2000, was published. Within the document, the term *critical information infrastructure* is not mentioned. In its place, ISD 2000 used the term *most important objects for ensuring the information security of the RF.* In ISD 2000, there is a long list of these objects, grouped by different spheres of Russian society. The spheres are economics, domestic policy, foreign policy science and technology, spiritual life, information and telecommunication systems, defense, law enforcement and judicial spheres, and emergencies.

The list in the ISD 2000 is the first published list of the most important objects for ensuring RF information security, that is, objects of the CIIRF. The list is quite broad and almost all encompassing. Even though it is not a list of the critical information infrastructure, it provides a basis for the study of the how the Russian interpretation of *critical information infrastructure* has developed.

3.2 Bill for the Security of Critical Important Objects of Information Infrastructure 2006

The Bill for Ensuring Information Security of Critical Important Objects of Information and Telecommunications Infrastructure, hereinafter CIO Bill 2006 (FZP- 340741-4, 2006), was introduced in the State Duma in 2006. In the CIO Bill 2006, the critical information and telecommunications infrastructure of the RF is the set of all critical information and telecommunications infrastructure segments (FZP- 340741-4, 2006). It defines a critically important object of the information and telecommunications infrastructure as the following:

> an integral part of the critical infrastructure of the Russian Federation, the termination or malfunctioning of which could lead to an emergency or to significant negative consequences for RF's defense, security, international relations, economics, or infrastructure of the country, or for the livelihoods of people living in the territory concerned for a long period. (FZP- 340741-4, 2006)

The *critical segments* (i.e., the critically important objects of the information and telecommunications infrastructure of the RF) include (FZP- 340741-4, 2006):

- State Automated Elections System[1]
- information and telecommunications systems of state authorities
- automated control systems for Russian armed forces
- satellite systems used for management and for special purposes
- information and telecommunications systems of law enforcement agencies
- television and radio broadcasting and other systems for keeping the population informed
- national registers and reference databases
- backbone communication networks and general communication networks in areas that do not have reserve or alternative types of communication
- software and hardware complexes for communication networks
- information and telecommunications systems of finance, credit, and banking activities and for managing the extraction and transportation of oil, oil products, and gas
- information and telecommunications management systems for water supply, water, and hydraulic equipment
- information and telecommunications systems for power supply management
- information and telecommunications systems of transport management
- information and telecommunications management systems for potentially hazardous facilities
- systems of prevention and mitigation of emergency situations
- geographic and navigation systems

According to the CIO Bill 2006, systems that do not relate to the above, but the violation of which may pose a threat to the national interests of the RF in information space, are also considered critical segments of the information and telecommunications infrastructure.

After two years of debate, the CIO Bill 2006 (FZP- 340741-4, 2006) was withdrawn in 2008. Even though it did not become law, the list of the critical segments provides insight into the Russian conception of the critical information infrastructure. Compared with the list of the most important objects for ensuring RF information security in ISD 2000, the list in the CIO

[1] Development of the State Automated Elections System, called *GAS Vybory*, started in 1994 and was first used during elections in 1995.

Bill 2006 is shorter. This list also concentrated more on the capability to act of state authorities and armed forces, the functioning of communication networks in all circumstances, and industry and logistics.

3.3 Policy Directions of Security of Critical Information Infrastructure 2012

In February 2012, Russian President Dmitry Medvedev approved a document called Main Directions of State Policy in Security of Automatic Control Systems for Production and Technology Processes in Critical Important Infrastructure Objects of the RF (SBRF, 2012), hereinafter CII Policy Directions 2012. The document complements the RF National Security Strategy in information security and in the protection of critical information infrastructure. CII Policy Directions 2012 is a document from the Security Council of the Russian Federation (SCRF). The Federal Security Service of the Russian Federation (FSB) was the main drafter of CII Policy Directions 2012. In addition, responsibility for a large part of the implementation of the measures described in the document lies with the FSB (Lavrentieva, 2012). CII Policy Directions 2012 defines both critical information infrastructure and critically important objects of the infrastructure of the RF, giving the following definition for the latter:

> a complex of automated systems for managing the critically important objects and for enabling their connections with the information and telecommunications networks, and which are used for the state management, to ensure the defense capability, security and law and order, and the violation (or termination) of which may cause of severe consequences. (SBRF, 2012)

A critically important object of the infrastructure of the RF is defined as

> an object, the violation (or termination) of functioning of which results in loss of management, destruction of infrastructure, irreversible negative change (or destruction) of the economy of the Russian Federation or administrative-territorial unit or a substantial deterioration of the safety of vital activity of the population residing in these territories for a long period. (SBRF, 2012)

From the Russian point of view, CII Policy Directions 2012 was a good guidance document, requiring the establishment of a system for early warning and detection of cyberattacks against critical infrastructure.

In CII Policy Directions 2012, CIIRF is officially defined for the first time even though the document does not contain a list of the critically important objects. Earlier, in ISD 2000, a term with the same meaning was the *most important objects for ensuring the information security of the RF*. The term *critical information and telecommunications infrastructure of the RF* was introduced in the CIO Bill 2006 (FZP- 340741-4, 2006) but the bill was never accepted in the State Duma.

3.4 CII Security Bill 2013

In 2013, five years after the CIO Bill 2006 was withdrawn, a bill called *On the Security of the Critical Information Infrastructure of the RF*, hereinafter the CII Security Bill 2013 (FZ-1, 2013), was introduced and submitted for public discussion. The critical information infrastructure of the RF is defined in the bill as follows:

> a complex of automated systems for managing production and technological processes of critically important objects and enabling their connections with the information and telecommunications networks, as well as information systems and communication networks used for the administration of the state, to ensure defense, security and law and order (i.e., objects of the critical information infrastructure of the Russian Federation). (FZ-1, 2013)

In the CII Security Bill 2013, there is no list of the critically important objects or of the critical information infrastructure. A critically important object is defined generally in the bill as

> an object, the violation or termination of functioning of which may lead to a loss of economic management of the Russian Federation, a constituent entity of the Russian Federation or an administrative territorial unit, its irreversible negative change (destruction), or a significant decrease in the safety of the population. (FZ-1, 2013)

The CII Security Bill 2013 defined the rights, obligations, and responsibilities of Russian state actors and the subjects of critical information infrastructure in the management of information security. The bill also included criteria for the categorization of the critical information infrastructure. In the categorization, the importance of the object is evaluated on an economical, ecological or social basis, or based on how important the object is for Russia's defense capabilities or national security. As a result of the evaluation, the objects were divided into high-, medium-, or low-risk categories. The bill was planned to come into force January 1, 2015, but it was not passed by the State Duma.

3.5 Russian Military Doctrine of 2014

The Russian Military Doctrine of 2014 reflects the changing international political situation. Tenser relationships with the West and the impact of the war in eastern Ukraine have made the doctrine more belligerent than the Military Doctrine of 2010. The use of information and communication technology for military–political purposes is mentioned in the doctrine as a new factor posing a military danger to Russia. Another military danger to Russia is causing disorder in the CII, which is not defined. The objects of the CII are listed as follows:

- command and control systems
- command and control systems of the armed forces
- information infrastructure of strategic nuclear forces
- missile defense early warning system
- space surveillance system
- information infrastructure of nuclear weapon depots
- nuclear power plants
- command and control systems of nuclear industry
- command and control systems of chemical industry

The CII list in the Military Doctrine of 2014 is military oriented and not inclusive but provides a good impression regarding the critically important military objects of the CII.

3.6 Russia–China Cyber Security Pact 2015

The RF and China signed a bilateral cyber security pact to maintain information security in May 2015 (RCPact, 2015). The pact does not define CII, but there is a list of its objects. They are not specifically mentioned as Russian objects, but they are a good example of how Russia sees the CII. The objects of the CII in the RCPact 2015 are information systems and information and telecommunications networks of state authorities or information systems, information and telecommunication networks, and automated process control systems operating in the following areas:

- defense industry
- healthcare
- transport
- communications
- credit and finance sector
- energy sector
- fuel industry
- nuclear industry

- rocket and space industry
- mining industry
- metallurgical industry
- chemical industry

An information system is a complex of information stored in databases and the information technology and technical means to process information. An information and telecommunication network is a technological system for transmitting information over communication lines, access to which is carried out using computer technology. An automated control system for technological processes is a complex of hardware and software designed to monitor and control technological and/or production equipment and technological and/or production processes implemented by such technological and/or industrial equipment (RCPact, 2015).

3.7 Information Security Doctrine 2016

In December 2016, President Putin signed the new Information Security Doctrine, hereinafter ISD 2016, which emphasized the need to ensure the stable and uninterrupted operation of the CIIRF. In the previous version of the document, ISD 2000, this aspect of information security was not given as much attention. This new focus relates to the continuously increasing number of threats to information security of critical objects (UP-646, 2016). The CIIRF is mentioned in ISD 2016 seven times but without definition. The information infrastructure of the RF is defined in ISD 2016 as

> a complex of the objects of informatization, information systems, sites in the “Internet” network and networks located in the territory of the Russian Federation, and in territories under the jurisdiction of the Russian Federation or used based on international treaties of the Russian Federation. (UP-646, 2016)

ISD 2016 is the first official Russian information security document to state that one of the national interests of the RF in the information sphere is ensuring the stable and uninterrupted functioning of the CIIRF and the unified telecommunications network of the RF in peacetime, during the threat of aggression, and in wartime. The CIIRF is mentioned as a target of technological influence for military purposes (UP-646, 2016).

3.8 CII Security Law 2017

The FSB started to draft a new bill of CIIRF security after the CII Security Bill failed to pass the State Duma in 2013. The CII Security Bill was introduced in the State Duma in 2016. The purpose of the bill was to define the organizational and legal basis of the information security management of the CIIRF to ensure its stable functioning when targeted by cyber attacks. The CIIRF was defined in the CII Security Bill as “a complex of critical information infrastructure objects, as well as telecommunication networks used to organize the interaction of critical information infrastructure facilities among themselves” (FZ-47571-7, 2017). The CII Security Bill also contains a list of the objects of the CIIRF. The list is the same as the list in the Russia–China Cyber Security Pact.

After three hearings and some changes to the draft of the CII Security Law, the State Duma adopted and the Federation Council approved the Bill of CIIRF security in July 2017. President Putin signed the Bill on the Security of the Critical Information Infrastructure of the RF, hereinafter the CII Security Law, in July 2017 (FZ-187) and it will enter into force at the beginning of 2018. In the CII Security Law, the CIIRF is defined as “objects of critical information infrastructure, as well as telecommunication networks used to organize the interaction of these objects” (FZ-187, 2017). The objects of the CIIRF are then defined as “information systems, information and telecommunication networks, and automatic control systems of the subjects of the critical information infrastructure” (FZ-817, 2017).

The subjects of the CIIRF are state organs and agencies, state institutions, Russian legal entities and private entrepreneurs who own or have in their possession, by other legal means, information systems, information and telecommunication networks, and automated control systems of technological processes operating in the following areas:

- defense industry
- healthcare
- transport
- communications
- credit and finance sector
- energy sector
- fuel industry
- nuclear industry
- rocket and space industry
- mining industry
- metallurgical industry
- chemical industry

The list is same as the one in the Russia–China Cyber Security Pact 2015.

4. Conclusions

The concept of the CIIRF has been developing since 2000 when the first Information Security Doctrine was published. The ISD 2000 was the first official document to discuss the idea of the CIIRF, but it failed to mention the term itself. In place of the term *critical information infrastructure*, ISD 2000 used, without a definition, the term *the most important objects for ensuring the information security of the RF.* ISD 2000 and its list of the most important objects for ensuring the information security of the RF were drafted at the end of the 1990s, when the international political situation was less tense than it is today. The list of these most important objects was broad, fragmented and included many that have not been reiterated in later versions of the critically important objects list of critical information infrastructure (CIO list of CII). After ISD 2000, the CIO lists have been more focused on security and defense.

In the CIO Bill 2006, the concept of the CIIRF was not defined. The most important objects for ensuring information security of the RF listed in the ISD 2000 were now called “critically important objects (CIO) of the information and telecommunications infrastructure which affect the security of the state in information space.” A CIO was defined as an object that, when its functioning is violated, it can lead to an emergency or to significant negative consequences for defense, security, international relations, the economy of the RF, or infrastructure of the country, or for the livelihoods of people living in the territory concerned for a long period. The CIO Bill 2006 included a list of CIOs focused more on security and defense than the list in ISD 2000. One interesting detail is that the first critical segment of the information and telecommunications infrastructure of the RF listed is the State Automated Elections System.

CII Policy Directions 2012 contained the first official definition of the CIIRF. According to that document, the CIIRF is a complex of automated systems for managing critically important objects (CIOs) and for enabling their connections with information networks. These objects are used for state management and for ensuring defense capability as well as security and law and order, and their violation may have severe consequences.

The deterioration of relations between Russian and the United States has also had an influence on CII Policy Directions 2012. In the document, the definition of the CII is security oriented. The main activities of the CII are state management, defense, and maintaining law and order. The economy is a new CIO of CII in CII Policy Directions 2012.

The CIIRF is defined in the CII Bill 2013 in the same way as it was defined in Policy Directions 2012. The only addition to the definition provided in the latter document is the automated systems for managing production and technological processes of critically important objects. In the CII Bill 2013, there is no definition of CIO of the CIIRF. The CIO is generally defined in the same way as the CIO of CIIRF was defined in CII Policy Directions 2012. Even though the CII Bill 2013 was not passed in the State Duma, the bill confirms that the concept of the CIIRF found its present form at the beginning of the 2010s.

After considering two versions of a bill for the security of the critical information infrastructure of the RF (2006 and 2013), the State Duma finally passed the third version in July 2017. The CII Security Law 2017 defines the CIIRF more simply than it had been defined in previous documents. According to the definition of the CII Security Law 2017, the CIIRF consists of "objects of critical information infrastructure, as well as telecommunication networks used to organize the interaction of these objects and the objects of the CIIRF are information systems, information and telecommunication networks, and automatic control systems of the subjects of the critical information infrastructure."

The CIO of CII is not defined, but the CII Security Law 2017 does contain a list of the objects of critical information infrastructure, including information systems, information and telecommunication networks of state authorities and the most important industrial sectors of and societal activity. The definition of CIIRF and the objects of CIIRF in the CII Security Law 2017 are the results of a long assessment and they can be considered as stable, long-term definitions.

For future research, the protection of the CIIRF is one fruitful area to consider. Another CIIRF-related topic for study is a comparison of how the concept of critical information infrastructure has developed in Russia and in Western countries. A third interesting framework for study is the hypothesis that the list of objects of the CIIRF is also a target development list for offensive cyber activities by Russia. For example, the State Election System was the first object on the list of the CIO Bill 2006, but has not been mentioned since that time.

Table: Critical Information Infrastructure (CII) and Critically Important Object (CIO) of the CII

Document	**Definition of CII and CIOs**
ISD 2000	**Critical information infrastructure of the Russian Federation**: not defined **Most important objects for ensuring the information security of the Russian Federation**: not defined but a list is included
CIO Security Bill 2006	The **critical information and telecommunications infrastructure of the RF** is the set of all critical information and telecommunications infrastructure objects A **critically important object of the information and telecommunications infrastructure** is an integral part of the critical infrastructure of the Russian Federation, the termination or malfunctioning of which could lead to an emergency or to significant negative consequences for RF's defense, security, international relations, economy, or infrastructure, or for the livelihoods of people living in the territory concerned for a long period.
Policy Directions of Security of CII 2012	The **critical information infrastructure of the RF** is a complex of automated systems for managing the critically important objects and for enabling their connections with the information and telecommunications networks, and which are used for the administration of the state and for ensuring defense capability as well as security and law and order, the violation (or termination) of which may cause of severe consequences. A **critically important object of the infrastructure of the RF** is an object the violation (or termination) of functioning of which results in loss of control, destruction of infrastructure, irreversible negative change (or destruction) of the economy of the RF or administrative-territorial unit or substantial deterioration of the safety of the population residing in these territories for a long period.
CII Security Bill 2013	The **critical information infrastructure of the RF** is a complex of automated systems for managing production and technological processes of critically important objects and enabling their connections with the information and telecommunications networks as well as information systems and communication networks used for state management and for ensuring defense as well as security and law and order (i.e., objects of the critical information infrastructure of the RF). A **critically important object** is an object, the violation or termination of functioning of which may lead to the loss of economic management and / or ensuring the defense capability, security and law and order of the RF, a constituent entity of the RF or an administrative territorial unit, its irreversible negative change (destruction) or a significant decrease in the safety of the population.
CII Security Law Draft 2017	**The critical information infrastructure of the RF** is a complex of critical information infrastructure objects as well as telecommunication networks used to organize the interaction of critical information infrastructure facilities among themselves. **Critically important objects of the critical information infrastructure**: no definition but a list is included
CII Security Law 2017	The **critical information infrastructure of the RF** is comprised of critical information infrastructure objects as well as of the telecommunication networks used to organize the interaction of these objects. **Objects of critical information infrastructure** are information systems, information and telecommunication networks, and automatic control systems of the subjects of the critical information infrastructure.

REFERENCES

Demidov, O. (2013). Киберкомандование США: уроки для России. Accessed March 31, 2017 http://www.perspektivy.info/rus/konturi/kiberkomandovanije_ssha_uroki_dla_rossii_2013-11-15.html

FZ-149. (2006). Федеральный закон об информации, информационных технологиях и о защите информации. Accessed March 16, 2017 http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108264

FZ-187 (2017). Федеральный закон о безопасности критической информационной инфраструктуры Российской Федерации. Accessed September 2, 2017 https://rg.ru/2017/07/31/bezopasnost-dok.html

FZP- 340741-4. (2006). Федеральный закон об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры. Accessed March 28, 2017 http://xn----9sbmabrf5adsldy9e3b.xn--p1ai/bill/340741-4

FZP-1. (2013). Федеральный закон о безопасности критической информационной инфраструктуры Российской Федерации - проект. Accessed March 28, 2017 http://rg.ru/pril/article/83/27/52/zakonoproekt.doc

FZP-47571-7 (2017). Федеральный закон о безопасности критической информационной инфраструктуры Российской Федерации - проект. Accessed March 28, 2017 http://asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=47571-7

Lavrentjeva, N. (2012). CNews. В России разработали государственную политику кибер-защиты. Accessed July 9, 2016 http://www.cnews.ru/news/top/v_rossii_razrabotali_gosudarstvennuy

MORF. (2011). Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. Accessed March 5, 2017 http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle#1

RBRPact. (2013). Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности, 25 декабря 2013 года, Москва. Accessed May 27, 2016 http://www.pravo.by/main.aspx?guid=3871&p0=A01300055&p1=1

RCPact. (2015). Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности, 8 мая 2015 года, Москва. Accessed May 27, 2016 http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWc_ABDJw.pdf

SBRF. (2000). Доктрина Информационной безопасности Российской Федерациию (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000, № Пр-1895. Accessed December 6, 2015 http://www.scrf.gov.ru/documents/5.html

SBRF. (2011). Конвенция об обеспечении международной информационной безопасности (концепция). Accessed March 31, 2017. http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

SBRF. (2012). Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации". (утв. Президентом РФ 03.02.2012 N 803 3.2.2012. Accessed March 17, 2016 http://www.consultant.ru/document/cons_doc_LAW_150730/

UP-646. (2016). Об утверждении Доктрины информационной безопасности Российской Федерации от 5 декабря 2016 г. № 646. Accessed March 31, 2017 http://kremlin.ru/acts/bank/41460

UP-203. (2017). Указ Президента Российской Федерации О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы от 09.05.2017 г. № 203. Accessed December 06, 2017 http://www.kremlin.ru/acts/bank/41919

III

THE PROTECTION OF RUSSIA'S CRITICAL INFORMATION INFRASTRUCTURE

by

Kari, M. (2018)

ECCWS 2018: Proceedings of the 17th European Conference on Cyber Warfare and Security (Oslo, 2018), pp. 533–540

Martti J Kari
PhD student
Faculty of Information Technology
University of Jyväskylä, Finland
Martti.j.kari@jyu.fi

THE PROTECTION OF RUSSIA'S CRITICAL INFORMATION INFRASTRUCTURE

The concept of the critical information infrastructure of the Russian Federation (CIIRF) has been in development for two decades. Together with this development there has also been constant debate on how the CIIRF should be protected. The core question of this debate has been the roles and responsibilities of different state authorities in information security (IS) management. Defining the CIIRF took almost two decades partly because of the power struggle over IS management between the Federation Security Service (FSB) and the Federal Service for Technical and Export Control (FSTEC).

The Information Security Doctrine of the Russian Federation 2016 defines one of the national interests in the information sphere to be ensuring the sustainable and uninterrupted functioning of the CIIRF. The doctrine, however, fails to define what the CIIRF is and which authorities should protect it. However, the CII Security Law, passed in July 2017, finally defines what objects constitute the CIIRF. Then, in November 2017, the FSTEC was named as the authority responsible for protecting the CIIRF. In 2012, the FSB was tasked with establishing a system, called GosSOPKA, for the detection and prevention of cyber-attacks, and in 2017 with operating the GosSOPKA system.

My research question is the following: How is the critical information infrastructure of the Russian Federation protected? The research method is grounded theory. The study is based on official Russian documents related to IS, including legislation and presidential decrees as well as documents of the Russian Federation Security Council, the FSB and the FSTEC.

My conclusion is that the definition of the CIIRF and the division of responsibilities to protect the CIIRF were confirmed by the legislation passed at the end of 2017. The next phase in the protection of the CIIRF, starting in 2018, is the implementation of these principles.

Keywords: Russia, Critical Information Infrastructure, Cyber threat; FSTEC, FSB, GosSOPKA

1. Introduction

The concept of the CIIRF was officially discussed for the first time in the Information Security Doctrine of the Russian Federation in 2000, hereinafter ISD 2000. The list of the objects of the CIIRF was long and included many that have not been reiterated in later versions of the list defining the critical information infrastructure (CII). However, this document did not clearly and unambiguously describe the ideas of protecting the CIIRF and the responsibilities and division of labor between state authorities. ISD 2000 was the beginning of a long debate about the protection of the CIIRF. The core question of this debate has been the roles and responsibilities of different state authorities in IS management at the state-level. To define and organize the protection of the CIIRF took almost two decades partly because of the power struggle over IS management between the Federation Security Service (FSB), the Federal Service for Technical and Export Control (FSTEC) and the Russian Armed Forces, and partly because of the clarification of the responsibilities of private companies and other legal entities for protection.

In February 2012, President Medvedev approved the document Main Directions of State Policy in the Security of Automatic Control Systems for Production and Technology Processes in Critical Important Infrastructure Objects of the RF (SBRF, 2012), hereinafter CII Policy Directions 2012. CII Policy Directions 2012 required the establishment of a system for the early warning and detection of cyber-attacks against critical infrastructure. In CII Policy Directions 2012, the FSB was tasked with establishing a unified state system of detection and warning for computer attacks on CII.

In January 2013, President Putin signed the decree on the creation of the state system for detecting, preventing and eliminating the consequences of computer attacks on the information resources of the Russian Federation, hereinafter the GosSOPKA[1] Decree (UP-31, 2013). The GosSOPKA system is a combined, territorially distributed complex that includes forces and means for detecting, preventing and eliminating the consequences of computer attacks and responding to computer incidents. The information resources of the Russian Federation are understood as information systems, information and telecommunications networks and automated management systems located in the territory of the Russian Federation as well as in the diplomatic missions and consular offices of the Russian Federation.

The Information Security Doctrine of the Russian Federation 2016 (UP-646, 2016) defines one of the national interests in the information sphere to be ensuring the sustainable and uninterrupted functioning of the CIIRF. The doctrine, however, fails to define the concept of the CIIRF and the authorities protecting it.

After considering two versions of a bill for the security of the CIIRF, one in 2006 and the other in 2013, the State Duma finally passed the CII Security Law in July 2017. The bill was drafted by the FSB and introduced in the State Duma in 2016. In July 2017, President Putin signed On the Security of the Critical Information Infrastructure of the Russian Federation (FZ-187, 2017), hereinafter the CII Security Law. The CII Security Law entered into force at the beginning of 2018. Its purpose is to define the organizational and legal basis of the IS management of the CIIRF to ensure its stable functioning when targeted by computer attacks.[2]

The CII Policy Direction 2012 and the GosSOPKA Decree of 2013 assigned the IS management related to cyber-attacks to the FSB, but the question of the comprehensive protection of the CIIRF remained unresolved until the CII Security Law in 2017.

As a discipline, computer science and information systems attempts to understand and explain information systems. In this article, I view CIIRF as an information system and my aim is to understand and examine how it is being protected. I begin by outlining a definition of the CIIRF. I then describe the principles of protection for the CIIRF and the roles of the FSB and the FSTEC in that protection, the categorization of objects that comprise the infrastructure, and the introduction and integration of GosSOPKA as a tool for its protection.

It should be noted that the idea to disconnect the Russian internet, the RuNet, from the global internet (Ristolainen, 2017) as a method of protecting the CIIRF is beyond the scope of this paper. The reason for this exclusion and limitation is that elements of the CIIRF are located beyond the boundaries of the RuNet and for this reason its disconnection would not protect them. Another reason is that threats to the CIIRF can also originate from inside the RuNet, in which case disconnection would not protect the critical infrastructure.

Methodologically, my paper is a literature survey. Primary sources include the Russian Federation’s laws and presidential decrees. Secondary sources and supporting material include commentary by Russian ICT specialists on the protection of the CIIRF.

2. The Critical Information Infrastructure of the Russian Federation

CII Policy Directions 2012 defines both the critical information infrastructure and the critically important objects of the infrastructure of the Russian Federation, providing the following definition for infrastructure:

[1] GosSOPKA is an abbreviation of the Russian phrase “state system for detecting, preventing and eliminating the consequences of computer attacks”.

[2] A computer attack is defined as the targeting of software and/or hardware in CII facilities, telecommunication networks used to organize the interaction of such objects, with a view to violating and/or terminating their operation and/or creating a security risk that is handled by such objects information.

> a complex of automated systems for managing the critically important objects and for enabling their connections with the information and telecommunications networks, and which are used for state management, to ensure the defense capability, security and law and order, and the violation (or termination) of which may have severe consequences. (SBRF, 2012)

A critically important object, meanwhile, is defined as the following:

> an object, the violation (or termination) of functioning of which results in loss of management, destruction of infrastructure, irreversible negative change (or destruction) of the economy of the Russian Federation or administrative-territorial unit or the substantial deterioration of the safety of vital activity of the population residing in these territories for a long period. (SBRF, 2012)

In December 2016, President Putin signed the new Information Security Doctrine, hereinafter ISD 2016. The ISD 2016 is the first Russian IS document to state that one of the national interests of the RF in the information sphere is ensuring the stable and uninterrupted functioning of the CIIRF and the unified telecommunications network of the Russian Federation in peacetime, during the threat of aggression, and in wartime. The CIIRF is mentioned as a target of technological influence for military purposes (UP-646, 2016). In ISD 2016, the information infrastructure of the Russian Federation is defined as

> a complex of the objects of informatization, information systems, sites in the “internet” network and networks located in the territory of the Russian Federation, and in territories under the jurisdiction of the Russian Federation or used based on international treaties of the Russian Federation. (UP-646, 2016)

The CII Security Law (FZ-187, 2017) defines the CIIRF more simply than it had been defined in previous documents:

> The CIIRF consists of objects of the critical information infrastructure as well as the telecommunication networks used to organize the interaction of these objects. The objects of the CIIRF are information systems, information and telecommunication networks, and automatic control systems of the subjects of the critical information infrastructure. (FZ-187, 2017)

The subjects of the CIIRF are state organs and agencies, state institutions, Russian legal entities and private entrepreneurs who own or have in their possession, by other legal means, information systems, information and telecommunication networks, and automated control systems of technological processes operating in the following areas:

- defense industry
- healthcare
- transport
- communications
- credit and finance sector
- energy sector
- fuel industry
- nuclear industry
- rocket and space industry
- mining industry
- metallurgical industry
- chemical industry

An automated control system is a set of software and hardware designed to control the technological and production equipment (actuators) and the processes they produce, and to manage such equipment and processes.

According to the official Russian view, the CIIRF is a target of both external and internal cyber-threats, and these threats are increasing and becoming more complicated to respond to. In the Russian estimation, foreign states are trying to penetrate the CIIRF with malware and other means and methods of cyberwarfare. The purpose of this penetration includes cyber-espionage, the denial of access to information in the CIIRF, corruption of information, and attacking the stability of functioning of objects the CIIRF. Terrorists and extremists can also attack the CIIRF (UP-24, 2000; MORF, 2011; SBRF, 2013).

Even though the IS management of the CIIRF has been discussed in Russia since ISD 2000, the process and responsibilities for its protection were not explicitly and comprehensively defined until the CII Security Law in 2017. The protection of the CIIRF is based on the division of responsibilities and labor between the FSB and the FSTEC, on the categorization of CII objects, the introduction and integration of GosSOPKA as a tool to protect the CIIRF, and on establishing systems for the its security.

3. Protection of the Critical Information Infrastructure of the Russian Federation

3.1 Roles of FSTEC and FSB in protection of CIIRF

The Federal Service for Technical and Export Control of the Russian Federation (FSTEC) is a federal executive body charged with ensuring the security of the CIIRF, countering technical intelligence and the technical protection of information as well as a specially authorized body in the field of export control (UP-569, 2017). Its predecessor, the State Technical Commission of the USSR, was established in 1973. It was a permanent body for the protection of secret and official state information, preventing its loss through technical channels, and for counteracting the operations of foreign technical intelligence services in Russia (Brusnitsin, 2000).

In 1992, the commission was organized as the State Technical Commission under the President of the Russian Federation (UP-9, 1992). In 1999, it received the status of a federal executive body. The tasks of the commission were the technical protection of information of governmental, federal and local executive bodies; forecasting the development of the forces, means and capabilities of technical intelligence; identifying threats to IS; and counteracting technical intelligence as well as preventing the leakage of information through technical channels (UP-212, 1999). In 2004, the State Technical Commission of Russia was transformed into the Federal Service for Technical and Export Control (UP-314, 2004).

According to regulations (UP-1085, 2004), FSTEC is a federal executive body authorized to provide security (using non-cryptographic methods) for the information in the information and telecommunications infrastructure systems that have a significant impact on the state's security in the information sphere. These may include information systems and telecommunications networks functioning as part of Russia's critical infrastructure, on which any destructive information impacts may have significant negative consequences. FSTEC carries out its activities directly and through its territorial bodies. The FSTEC and its territorial bodies are part of the state security agencies (UP-1085, 2004).

In November 2017, the FSTEC was tasked with ensuring the security of the CIIRF and its significant objects. At the same time, it was also nominated to counter technical intelligence and provide technical protection of information as well as act as a specially authorized body in the field of export control (UP-569, 2017).

The Committee for State Security of Soviet Union, more commonly known as the KGB, was established in 1954. It was authorized to provide internal security and foreign intelligence, including signal intelligence (SIGINT). After the Soviet coup d'état attempt in August 1991, the KGB was divided into three organizations – the Foreign Intelligence Service (SVR), the Federal Counterintelligence Service (FSK) and the Federal Agency for Government Communications and Information (FAPSI). In 1995, the FSK was reorganized as the Federal Security Service (FSB). The FAPSI consisted of the KGB's 8th directorate (government communications) and 16th directorate (SIGINT). In 2003, FAPSI was reorganized into the Service of Special Communications and Information and the FSB took over the Special Communications and Information Service. The FSB also became responsible for SIGINT. The primary functions and roles of the FSB include law enforcement, counterintelligence, domestic surveillance, and internal intelligence functions at the national level. Cyber and internet surveillance is a new focus of FSB SIGINT collection efforts.

In IS management, the FSB is defined as the federal executive body authorized to ensure the functioning of the state system for detecting, preventing and eliminating the consequences of computer attacks on the information resources of the Russian Federation. In the protection of the CIIRF, the FSB's main task is to operate GosSOPKA, the state system of detection, prevention, and elimination of consequences of computer attacks on the information resources of the Russian Federation. (UP-620, 2017.)

3.2 Categorization of objects of CIIRF

The identification and categorization of the objects of the CII is the first step in the process to secure and protect the CIIRF. The categorization of these objects is a process during which a subject in the CIIRF evaluates and categorizes the significance of a CII object according to the instructions of the FSTEC. Significant objects are placed into Category I, II or III. The categorization (i.e. the assigning of a category number to each object) is based on the social, political, economic, environmental significance of the object for ensuring the country's defense, state security and law and order. Category I is for the CII's most significant objects.

Social significance depends on the potential damage that would result from the malfunctioning or disruption of the object in the following areas: the life or health of people, life support facilities, transport infrastructure, communication networks, and public services (FZ-187, 2017). For example, if the malfunctioning of an object is estimated to injure or cause death to less than 50 people, the object belongs to Category III. If the malfunctioning of an object might result in the injury or death of more than 500 people, the object belongs to Category I (PPP-0101, 2017).

The estimated possible domestic and foreign policy damage to the interests of the RF defines the political significance of an object in the case of the malfunction or stoppage of this object (FZ-187, 2017). For example, the official website of the president of the Russian Federation or the government belong to Category I, while the website of city or town administration belong to Category III (PPP-0101, 2017). Environmental significance is expressed by assessing the level of environmental impact. If a CII object does not meet the criteria of significance, it is not assigned to any of these categories (FZ-187, 2017).

The subject sends the results (i.e. information on the categorized objects) to the FSTEC, which approves the categorization and includes it in a registry of the significant objects of the CIIRF. An object receives the status of a significant CII object when it has been assigned to a category and it is included in the registry. The registry includes the names of significant objects and their subjects, information on the interaction between the object and the telecommunication network, category number, information about the software and hardware used in the object and measures used to ensure the security of a significant CII object. The FSTEC delivers the registry information to the FSB, which then uses the information in GosSOPKA (FZ-187, 2017).

After the categorization, FSTEC specifies requirements to ensure the security of critical CII objects and requirements to establish security systems and ensure the functioning of these objects. The FSTEC specifies requirements to ensure the security of information and telecommunications networks which are assigned to one of the three categories of significance and which are included in the registry of significant CII objects, in cooperation with the Ministry of Telecom and Mass Communications of the Russian Federation. In the banking and finance sector, the FSTEC specifies requirements in consultation with the Central Bank of the Russian Federation. The subject of the CII is obliged to follow FSTEC instructions and establish security arrangements corresponding to category of significance of the CII object. FSTEC is authorized to evaluate the security arrangements of the objects included in the registry.

3.3 GosSOPKA

In January 2013, President Putin tasked the FSB with establishing a state system for the detection, prevention and elimination of the consequences of computer attacks on the information resources of the Russian Federation. The system is called GosSOPKA. The information resources were defined as information systems and information and telecommunications networks of state authorities, along with other information systems and information and telecommunications networks located in Russian Federation territory as well as the country's diplomatic missions and consular offices abroad (UP-31, 2013). The main task of GosSOPKA is ensuring the security of the information resources of Russia from computer attacks and maintaining the stable functioning of these resources in the face of incidents caused by computer attacks (SBRF, 2014).

The FSB was also tasked with ensuring the functioning of elements of GosSOPKA in cooperation with other state authorities. The FSB determines the procedure for the exchange of information between federal executive authorities on computer incidents. Furthermore, it defines the measures to assess the degree of protection of the country's CII from computer attack and develops recommendations on how to protect it from such attacks (UP-31, 2013).

In December 2017, FSB was named (UP-620, 2017) as the state authority to operate GosSOPKA. The IS management processes implemented in the GosSOPKA framework are the following: detecting, attributing and responding to computer attacks; eliminating the consequences of computer attacks on the information resources of the Russia; estimating the IS management situation and cyber threats; and the collection and analysis of information about computer attacks and computer incidents (SBRF, 2014; UP-620, 2017). These processes also include the organization and implementation of cooperation between law enforcement agencies and other state bodies, owners of information resources, telecom operators and internet providers in the detection of computer attacks, the collection and analysis of information about such attacks and incidents, and the monitoring of the security level of information systems as well as information and telecommunication networks.

The FSB established and operates the National Coordination Center for Computer Incidents[3] (NCCCI) and regional and territorial IS operations centers (SOC). The GosSOPKA SOCs are to be established in the Russian Federation at the federal district[4] and subject level.[5] The SOCs can be operated by the FSB, or they can be departmental or corporative SOCs. Figure 1 presents the types and hierarchy of different SOCs. The common tasks of SOCs include collecting and analyzing information about computer attacks and computer incidents, responding to threats, and eliminating the consequences of computer incidents in information resources (UP-31, 2013).

The task of FSB SOCs is to protect the information resources of state organs and bodies as well as the information resources of Russian Federation subjects. At the administrative departmental level, a state body can establish a departmental center[6] to protect the information resources of an administrative branch or department. In addition to providing IS, departmental centers receive and collect information on security and incidents occurring in all subordinate organizations. Departmental centers also conduct analytics on the data obtained, identify common trends or actual vectors and transfer information about them to downstream centers. State corporations, telecom operators and other organizations that carry out licensed activities in IS can establish and operate corporative GosSOPKA centers to protect their own information resources.

[3] Национальный координационный центр по компьютерным инцидентам

[4] A federal district is a grouping of the federal subjects for the convenience of operation and governing by federal governmental agencies. There are eight federal districts in Russian Federation.

[5] The subjects of the Russian Federation are the main administrative divisions in Russia. The federal subjects are divided into oblasts, republics, krais, autonomous okrugs, federal cities and autonomous oblasts.

[6] ведомственный центр

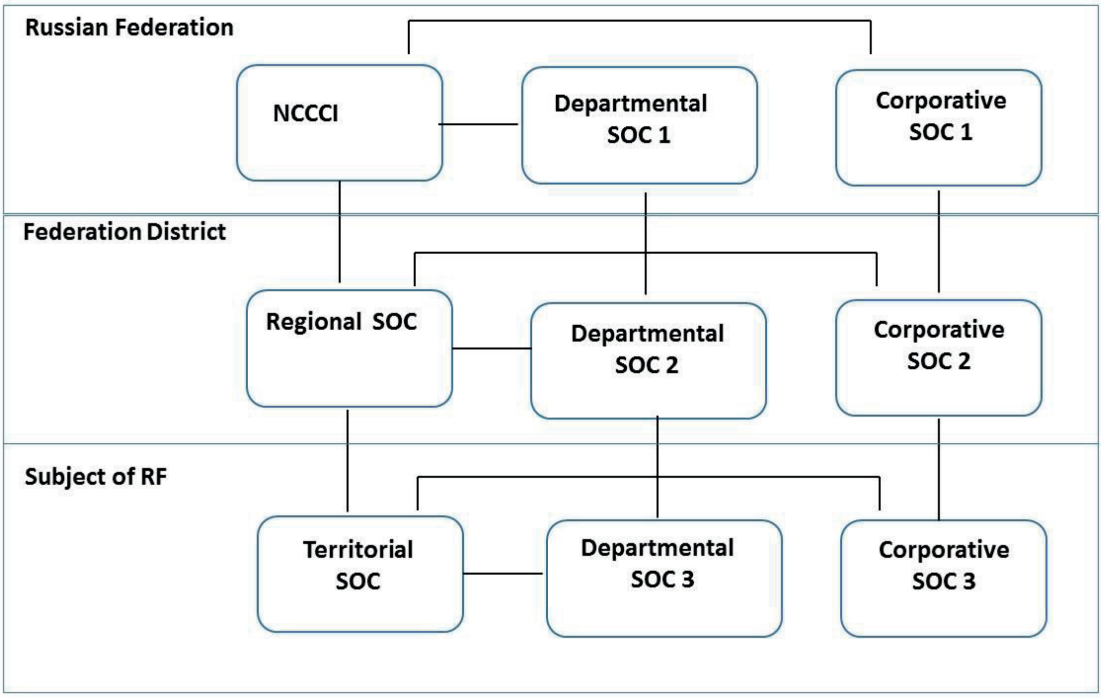


Figure 1. The types and hierarchy of SOCs

The first corporative and departmental GosSOPKA SOCs were established in 2016. In autumn of that year, the Russian state corporation Rostekh[7] established a corporative SOC. Rostekh develops, produces and exports high-tech civilian and military products. At the end of 2017, the Rostekh SOC was able to monitor 20% of the internet traffic of all companies and facilities belonging to the corporation. This means 386 enterprises and more than 24,000 external IP addresses. According to the plans, in 2020 about 30% of traffic is under SOC surveillance (Rostekh, 2017). The first departmental GosSOPKA SOC was established in 2016 in the Ministry of Economic Development. In summer 2017, the Ministry of Transport requested tenders to establish a departmental SOC by the end of 2018, and in autumn 2017, the Ministry of Foreign Affairs also issued a call for tenders on establishing a SOC (Voejkov, 2017).

Departmental and corporative centers can be established and operated by licensed commercial companies. For example, in November 2017 the companies Solar Security and Positive Technologies started a joint venture to create departmental and corporative GosSOPKA centers. Positive Technologies provides technological solutions, including information interaction with NCCCI, managing incidents, and detecting and blocking malware. Solar Security operates the centers established by Positive Technology (TAdviser, 2018).

3.4 CII subjects in the protection of CIIRF

The CII subjects are authorized to receive any information from the FSTEC that is necessary to ensure the security of significant CII objects, including security threats. The FSTEC delivers information to CII subjects about the means and methods of computer attacks as well as about the means and methods to prevent and detect those attacks. The subject is authorized, at its own expense, to purchase, lease, install and maintain GosSOPKA equipment and devices (FZ-187, 2017).

[7] State Corporation for Assistance to Development, Production and Export of Advanced Technology Industrial Product (Rostekh)

The subjects should immediately report computer attacks to the FSB, take measures to repel attacks and allow FSB officers to enter their facilities. In the case of an attack on the objects of the financial sector, the Central Bank also needs to be notified. The NCCCI coordinates the activities of the subjects to repel computer attacks. If GosSOPKA equipment is installed in the facilities of the CII subject, the subject is obliged to operate the equipment and maintain proper conditions for its use.

To ensure the safety of a significant CII object, the subject is obliged to establish a security system and to ensure its functioning according to the instructions of the FSTEC. The tasks of the security system of a significant CII object are to prevent unauthorized access to information and all illegal actions with respect to such information as well as the violation of information processing, to restore the functioning of critical objects, and continuous interaction with GosSOPKA. The FSB assesses the security of the CIIRF in order to predict the emergence of possible threats to its security and to develop measures to improve its stability when targeted by computer attacks. These assessments are based on the information received from GosSOPKA or from detection devices in telecommunication networks, from the FSTEC and from other authorities working with IS management (including foreign and international actors). They are also based on the information collected during the inspection and evaluation of significant CII objects. The FSB delivers the results of the assessments to the FSTEC, which maintains the registry of significant objects and makes planned as well as ad hoc inspections and evaluations. Ad hoc inspections are caused by, for example, a computer incident in a significant object (FZ-817, 2017).

4. Conclusions

The concept of the CIIRF has been in development since 2000, when the first Information Security Doctrine was published. Alongside this development, there has been an active debate about the roles and responsibilities of state authorities in IS management. After considering two versions of a bill for the security of the CIIRF (2006 and 2013), the State Duma finally passed the third version in July 2017. The CII Security Law 2017 extremely important for improving the effectiveness of ensuring cybersecurity of CIIRF. The Law defines the CIIRF more simply than in previous documents, starts the implementation phase of the protection of CIIRF.

Furthermore, the CII Security Law and related legislation defined the roles of two authorities in the IS management of the CIIRF. The FSB was tasked with creating and operating GosSOPKA, and the FSTEC was named as the federal executive body authorized to ensure the security of the CIIRF.

The definition of the CIIRF and the division of responsibilities to protect it were confirmed in legislation at the end of 2017. The next phase in the protection of the CIIRF, starting in 2018, is the implementation of these principles.

REFERENCES

Brusnitsin, N. Кто подслушивает президентов (От Сталина до Ельцина). *Who is wiretapping the presidents (From Stalin to Yeltsin)* – М.: Вита-Пресс, 2000. [online], http://www.connect-wit.ru/informatsionnaya-bezopasnost-gosudarstva-ot-gostehkomissii-sssr-do-fester-Rossii.html

FZ-187 (2017). Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации". *Federation Law Number 187 on the Security of Critical Information Infrastructure of the Russian Federation.* [online], https://rg.ru/2017/07/31/bezopasnost-dok.html

MORF (2011). Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. *Conceptual views on the activities of the Armed Forces of the Russian Federation in the information space* [online], http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle

Ristolainen, Mari. (2017). Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security Between Russia and the West. Journal of information warfare. Volume 16, Issue 4.
https://www.jinfowar.com/journal/volume-16-issue-4/should-%E2%80%98runet-2020%E2%80%99-be-taken-seriously-contradictory-views-about-cyber-security-between-russia-west

Rostekh. (2017). Ростех создал структуру для борьбы с киберугрозами. *Rostekh has created a framework for combating cyberthreats.* [online], http://rostec.ru/news/4519332

PPP-0101. (2017). Проект постановления Правительства РФ «Об утверждении показателей критериев значимости объектов КИИ РФ и их значений, а также порядка и сроков осуществления их категорирования». *Draft of the Decision of the Government of the Russian Federation "On the approval of indicators of the criteria for the significance of the objects of the CII RF and their meanings, as well as the procedure and deadlines for their categorization* [online], Проект 01/01/09-17/00073423

SBRF (2012) "Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации" (утв. Президентом РФ 03.02.2012 N 803), [online],
, [online], http://www.consultant.ru/document/cons_doc_LAW_150730/

SBRF (2013) "Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года*". Basics of the state policy of the Russian Federation in the field of international information security for the period until 2020*". [online], http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=178634&fld=134&dst=1000000001,0&rnd=0.5310172209117789#0

SBRF. (2014). Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом РФ 12.12.2014 N К 1274*). Extract from the Concept of the State System for Detection, Prevention and Elimination of the Consequences of Computer Attacks on Information Resources of the Russian Federation*. [Online], http://www.scrf.gov.ru/documents/6/131.html

UP-9. (1992). Указ Президента РФ от 5 января 1992 г. № 9 «О создании Государственной технической комиссии при Президенте Российской Федерации». *Decree of the President of the Russian Federation of January 5, 1992 No. 9 "On the establishment of the State Technical Commission under the President of the Russian Federation"* [online], https://www.lawmix.ru/pprf/98289

UP-31. (2013). Указ Президента Российской Федерации от 15 января 2013 г. N 31с г. Москва "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации*". Decree of the President of the Russian Federation of January 15, 2013 N 31c Moscow "On the establishment of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation".* [Online] https://rg.ru/2013/01/18/komp-ataki-site-dok.html

UP-314. (2004). Указ Президента Российской Федерации от 9 марта 2004 г. N 314 «О системе и структуре федеральных органов исполнительной власти». *Decree of the President of the Russian Federation of March 9, 2004 N 314 "On the system and structure of federal executive bodies".* [online], https://rg.ru/2004/03/11/federel-dok.html

UP-569. (2017). Указ Президента РФ от 25.11.2017 N 569 "О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. N 1085". *Decree of the President of the Russian Federation of 25.11.2017 N 569 "On Amendments to the Provisions on the Federal Service for Technical and Export Control, approved by the Decree of the President of the Russian Federation of August 16, 2004 N 1085".* [online], http://www.consultant.ru/document/cons_doc_LAW_283384/

UP-620. (2017). Указ Президента РФ от 22 декабря 2017 г. № 620 "О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации". *Decree of the President of the Russian Federation of December 22, 2017 No. 620 "On improving the state system for detecting, preventing and eliminating the consequences of computer attacks on the information resources of the Russian Federation."* [online], http://www.garant.ru/products/ipo/prime/doc/71740924/

UP-1085. (2004). Указ Президента РФ от 16 августа 2004 г. N 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (с изменениями от 22 марта, 20 июля 2005 г., 30 ноября 2006.). *Decree of the President of the Russian Federation of August 16, 2004 N 1085 "Questions of the Federal Service for Technical and Export Control" (as amended on March 22, July 20, 2005, November 30, 2006.)* [online], https://fstec.ru/component/attachments/download/234

Voejkov, Denis. (2017). Сверхсекретная ГИС ФСБ начала выходить из тени. *The top secret GIS of the FSB began to come out of the shadow* .http://www.cnews.ru/news/top/2017-10-06_sverhsekretnaya_gis_fsb_nachala_vyhodit_iz_teni

IV

STRATEGIC CULTURE THEORY AS A TOOL FOR EXPLAINING RUSSIAN CYBER THREAT PERCEPTION

by

Kari, M. (2019)

ICCWS 2019: Proceedings of the 14th International Conference on Cyber Warfare and Security (Stellenbosch, 2019), pp. 528–535

Strategic Culture Theory as a Tool for Explaining Russian Cyber Threat Perception

University Teacher, PhD student Martti J. Kari
University of Jyväskylä, Jyväskylä, Finland
martti.j.kari@jyu.fi

Abstract: The increasing interest in cyber warfare studies has created a need for theoretical tools to research the nature of cyber conflicts, cyber threats and the responses to these threats. One possible tool is the theory of strategic culture. According to Professor Alastair Iain Johnston, strategic culture is an integrated system of symbols, which establishes comprehensive and long-lasting strategic preferences. Strategic culture consists of basic assumptions about the strategic environment, including threat perception, as well as assumptions about the options to respond to the threats on an operational level. The theory of strategic culture identifies the factors that influence the formulation and outcome of strategic culture of a state. These factors may encompass historical, geographical, technological or political factors.

This paper argues that strategic culture theory is a suitable tool for exploring and explaining the Russian idea of cyber conflicts, the country's cyber threat perception and its strategic preferences, that is, its options to respond to cyber threats. This paper first identifies the specific factors influencing Russian strategic culture then moves on to a discussion of the elements comprising it. These elements, which can also be identified in the cyber environment, include a sense of vulnerability, the narrative of Russia as a besieged fortress, and Russia´s technological inferiority.

Methodologically, this paper is a literature survey, based on official Russian documents related to information security. These include the Russian Federation's information security doctrines, draft legislation and laws as well as documents from the RF Security Council and Ministry of Defense.

Keywords: Strategic Culture Theory, Russian Strategic Culture, Russian Cyber Threat Perception

1 Introduction

In recent years, cyberspace has become a domain of warfare. In June 2016, the NATO summit declared cyberspace as precisely that. According to Russian authorities, the formation of cyberspace as a warfare domain poses a threat to the Russian Federation's (RF) national interests (MORF, 2011; MD, 2014). The Stuxnet attack against Iranian nuclear facilities was the first example of new generation of warfare and showed that cyberweapons would be the "weapon of the century." A similar attack on Russian targets could cause enormous damage to Russia if it could not be countered. (Orlov, 2011.)

The increased interest in cyber threats has, in turn, heightened the need for theoretical tools to study the perceptions of those threats. However, cybersecurity studies are a relatively new field, so academic research of cyber threat perception has remained limited. The already existing research has concentrated on the system level and dealt, for example, with cybercrime (Bolden & Nalla, 2014) or the protection of information systems against cyber-attack (Zhuang et al, 2010). This paper argues that strategic culture theory is a suitable lens for explaining Russian cyber threat perception and the options to respond to such threats.

The basic assumption of the theory of strategic culture resides in the belief that all nations have their own kind of strategic culture, i,e. collective ideas and values, which are constitutive factors in the design and execution of states' security policies. Strategic culture consists of a central paradigm and a set of strategic preferences. The central paradigm describes the nature of the conflict and the perception of the enemy and threat as well as how to respond to that threat. Strategic preferences are assumptions about what options are the most effective against a particular threat (Johnston 1995a). Different states have their own strategic culture, developed over a long period. Factors influencing strategic culture might be historical, technological, political or organizational. Knowing these factors might be possible to explain how and why a state experiences a threat in a certain way. Strategic choices are based more on historically rooted strategic preferences than, for example, on changes in the strategic environment. If the strategic culture does change, it changes slowly (Johnston, 1995b).

Johnston (1995b) sees that one productive way to identify the elements of a nation's strategic culture is to analyze the content of recent subject-related texts. To explain the strategic culture related to the Russian perception of cyber threat, the most interesting texts are the Russian Federation's Military Doctrine (MD, 2014), Security Strategy (UP-683, 2015), Foreign Policy Concept (UP-640, 2016), Doctrine of Information Security (UP-646, 2016) and Strategy for the Development of an Information Society in the Russian Federation 2017-2030 (UP- 203, 2017).

Methodologically, this paper is a literature survey. It first identifies the specific factors influencing Russian strategic culture then moves on to a discussion of the elements comprising it. These elements, which can also be identified in the cyber environment, include a sense of vulnerability, the narrative of Russia as a besieged fortress and Russia's technological inferiority. In the end is described how the elements of Russian strategic culture and especially threat perception are reflected in the cyber environment and the strategic preferences Russian leadership has chosen to respond to those threats.

2 Theory of Strategic Culture

Gabriel Almond and Sidney Verba developed the concept of political culture in the 1960s. According to them, political culture is a "subset of beliefs and values of a society, which relate to the political system." (Almond & Verba, 1963.) In 1977, Jack L. Snyder brought political culture into security studies with his study *The Soviet Strategic Culture*. He identified historical, institutional, and political factors that had an influence on Soviet strategic thought, which he called "strategic culture." According to Snyder (1977), to understand the reactions of the Soviet Union one had to identify the factors influencing the Soviet strategic culture. After Snyder, the theory of strategic culture developed through three generations of scholars, each with their own conceptual and methodological approach. (Johnston, 1995a).

Professor Colin S. Gray was another important scholar of the first generation of the strategic culture school. He noted that the rational-actor theories were not able to explain the proxy wars in the Middle East and the US defeat in Vietnam. This caused a need to understand why states made strategic decisions and waged war in different ways in the same kinds of situation. Gray (1971) questioned the rational-actor theories as a tool to explain state behavior.

The second-generation scholars started to study the relationship between strategic culture and behavior. In the early 1980s, many researchers argued that the USA was incapable of thinking and acting strategically, and the Soviet Union, as a Clausewitzian and militarily oriented state, had an advantage vis-à-vis the USA. Some considered the USA weak and unable to challenge the authoritarian Soviet Union. These forecasts proved wrong. Researchers were not able to understand the internal and political changes in the Soviet Union well enough to predict its collapse at the beginning of the 1990s. This failure led to a new approach to strategic culture studies (Desch, 1998).

In the early 1990s, constructivism became one of the major schools in the study of international relations. In contrast to neorealism and neoliberalism, constructivism stressed that historical and social constructions are the basics of international relations. At the same time, strategic culture studies expanded beyond nuclear war, and were inspired by constructivism. One of the most important representatives of this third generation of strategic culture studies is Alastair Iain Johnston. His book *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History* (1995b) is considered a basic work of this new approach to the field (Lantis, 2006). Johnston studied the character and linkages of Chinese strategic culture to the use of military force against external threats. In his methodological framework, cultural orientations were the independent variable and military strategy was the dependent variable. He defined strategic culture as he following:

> *An integrated system of symbols (e.g. argumentation, structures, languages, analogies, metaphors) which acts to establish pervasive and long-lasting grand strategic preferences by formulating concepts of the role and efficacy of military force in interstate political affairs, and by clothing these conceptions with such an aura of factuality that the strategic preferences seem uniquely realistic and efficacious.* (Johnston, 1995b.)

Strategic culture (Johnston, 1995b) is a set of persistent and consistent historical patterns of how a state or state leadership thinks about the use of force to achieve political goals. Different states have different patterns of action and strategic preferences. The preferences originate in the historical experiences related to the threat and use of force by the state and are influenced by the philosophical, political, cultural, and cognitive experiences and characteristics of the state. Ahistorical and other variables – such as technology, capabilities, threat levels and organizational structure, which Johnston calls “objective variables” – have less influence on strategic preferences.

Johnston’s work has been criticized, especially because he distinguishes strategic culture from strategic behavior. Johnston isolates strategic culture as an independent variable and measures its causality to state behavior. Yet one of Johnston’s critics, Colin Gray (1999), stated that strategic behavior cannot be isolated from strategic culture, and that it is more important to understand strategic behavior than it is to explain it. Therefore, the theory of strategic culture should try to interpret the meaning of strategic behavior than it is to explain the cause of that behavior. According to Johnston, strategic culture is an independent and isolatable variable which causes the behavioral choices of states. In Johnston’s model, causality moves from culture to behavior.

If strategic culture does change, it changes slowly. Three factors shaping strategic culture are external shock, conflict of strategic principles and the behavior of the elite. An external shock can overturn a nation’s historical narratives and construct new norms. The second factor that may change strategic culture is disharmony and a clash of the core principles of strategic thinking. A third factor that can change strategic culture is the role of elites. Leaders can follow the current direction of their foreign policy, that is, their strategic culture or they can change their strategic culture by adopting a new approach to foreign policy questions (Lantis, 2006).

In this paper, I apply Johnston’s definition of strategic culture and his methodological framework. The factors influencing Russian strategic culture are considered independent variables. The central paradigm and strategic preferences of Russian strategic culture are then viewed as dependent variables. This paper follows Johnston’s idea about the separation of strategic culture (i.e., its central paradigm and strategic preferences) from state behavior in practice. Russian state behavior in the cyber environment in practice is difficult to explore, but the central paradigm and strategic preferences can be found in Russian official documentation.

Strategic culture is not an autonomous concept. Instead, it consists of a series of debates regarding its nature, the bearers of the concept, and its factors and elements. Some researchers see that the notion of a unitary strategic culture should be questioned and it would wiser to think of strategic culture as an umbrella concept for different subcultures (see Murray, 1999; Gray, 2006; Zaman, 2009). For example, within military organizations there will be separate subcultures influenced by traditions and the mission they perform (Murray, 1999; Gray, 2006).

The identified advantages and disadvantages of strategic culture theory have varied for several reasons. First, scholars of strategic culture theory from different generations vary in their definition of strategic culture and its content. Second, scholars of strategic culture and scholars representing traditional actor theories have viewed the concept differently (Horton-Eddison, 2018). The main advantage of strategic culture theory is in how it defines and describes components of a strategic culture (i.e., its central paradigm and strategic preferences), both of which are easier to identify and describe than unstructured state behavior. Another advantage is that strategic culture considers state-specific factors which influence state behavior. One disadvantage is that among scholars there is no common view of what the independent and dependent variables of strategic culture are.

Even though strategic culture can be criticized (see, e.g., Horton-Eddison, 2018; Lock 2018) as a vaguely defined concept with logical inconsistencies, it can also be used as a tool for providing framework and context. In this paper, the context it provides promotes a better understanding of how Russian strategic culture constructs an umbrella concept for the subculture related to Russian cyber defense. It explains Russian cyber threat perception and the response to that threat as the components of Russian cyber subculture.

3 Factors Formulating Russian Strategic Culture

One of the basic questions of the theory of strategic culture is the question of independent variables, those factors that influence strategic culture. These factors might be historical, geographical, and political or they can relate to organization or technology. Historical factors have a predominant influence on the formulation and outcome of a state's strategic culture. These historical factors are, in turn, influenced by the political, cultural and cognitive characteristics of the state. Technology, threat level and organizational structures – so-called "ahistorical or objective variables" – are of secondary importance. In Johnston's view (1995b), strategic choices are based on historically rooted strategic preferences.

This paper composes the factors that influence Russia's strategic culture into four groups: history, geography, technology, and the political system and worldview of Russian leadership. Disharmony and a clash of the core principles of strategic thinking can also have an influence on strategic culture. In addition to the four groups of factors, this paper discusses the "changed rules of war," which also have an influence on Russian strategic culture.

Russia has been attacked many times throughout its history, and this historical experience is an important factor of the country's strategic culture. Mongols destroyed Kiev in 1240 and ruled until 1380. After that, Russia has been attacked by Sweden in 1700 and Napoleon in 1812. Germany attacked Russia in both World Wars. The German invasion in the Second World War was particularly traumatic, causing enormous casualties to the Soviet population and significant damage to the country's infrastructure. These historical experiences, along with NATO expansion (Facon, 2016; Eitelhuber, 2009), has created a sense of vulnerability and a fear of invasion combined with the concept of Russia as a besieged fortress.

During the time of troubles (1606–1613), internal disturbances and foreign intrusion devastated many cities and depopulated rural regions. In the 17th century, there were numerous riots and uprisings throughout the country. In 19th century there were uprisings in Poland and, in 1825, the so-called Decembrists tried to organize a coup d'état in St. Petersburg. Two further revolutions eventually crushed the tsarist regime and brought the Communists to power. The breakup of the Soviet Union was yet another traumatic historical incident for the Russian people (Ermarth, 2006; Eitelhuber, 2009).

Geography has exerted a continuing influence on Russia’s threat perceptions. The East European Plain between the Carpathians and Ural mountains has been an easy area for attackers to advance across. The absence of natural physical buffers and barriers to protect the country from attack has increased Russians’ feeling of vulnerability (Ermarth, 2006; Facon, 2016).

Russia’s technological inferiority, particularly its backwardness in the development of high technology, has also had an influence on the country’s strategic culture. In its Information Security Doctrine, this technological backwardness is admitted indirectly. The Doctrine states also that some states try to dominate the information space by using their technological superiority, which can unbalance strategic stability. This imbalance is why one of the main tasks to ensure information security is to make Russian information technology competitive and develop the country's scientific and technological capability in information security (UP-646, 2016).

Even though the central paradigm of Russian strategic culture has remained unchanged for centuries, disharmony and the clash of core principles of strategic thinking have influenced the role of conflict, the country’s threat perception, and its strategic preferences in the 2010s. This outlook was revealed by General Gerasimov in 2013, when he stated that the rules of war have changed. The role of nonmilitary means to achieve political and strategic goals has grown, and, in many cases, these means have exceeded the power of weapons in their effectiveness. The lines between war and peace have been blurred. Wars are no longer declared and they proceed according to an unfamiliar template.

According to the Military Doctrine 2014, a range of elements characterizes modern conflict. These include the integrated use of military force with political, economic, and informational as well as other non-military measures; the use of special operations forces; and influencing the enemy throughout its territory simultaneously in the global information space, aerospace, land and sea. As characteristics of modern warfare, the Doctrine also includes the use of indirect and asymmetric methods and externally funded and run political opposition and social movements. The concept of the permanent war zone is also introduced in the Doctrine.

4 Elements of Russian Strategic Culture

The foundational elements of strategic culture are derived from the factors informing that culture. Together, these elements form a nation’s strategic culture: its central paradigm, which defines the nature of the conflict, enemy and threat, and its strategic preferences, which includes those operational-level assumptions of how to respond to that threat. The Military Doctrine of the RF, published in 2014, reflects the main elements of Russian strategic culture. It describes the nature and role of the conflict as well as the enemy and the threat posed by that enemy. The Doctrine divides an adversary’s possible activities against Russia into two components: danger and threat. A military danger is a state of interstate or domestic relations characterized by a set of factors that could, under certain conditions, lead to a military threat. A military threat is a state of interstate or domestic relations characterized by the possibility of a military conflict between the opposing sides. The Military Doctrine names NATO as one of the main external military dangers. The danger consists of NATO’s overall capacity, the organization’s potential violations of international law, and the encroachment of its military infrastructure on Russia’s borders (MD, 2014).

The Kremlin sees the international arena as a dangerous, chaotic, and volatile battlefield (Sinovets, 2016), where the battle to disrupt Russia’s digital sovereignty is waged every day. According to President Putin (2015), the aim of the United States is “to destroy strategic balance, to change the balance of power in such a way not just to dominate but to dictate their will to anyone.” In the Russian view, the USA uses its technological superiority to dominate the information space (UP-646, 2016). Digital sovereignty[1] means Russia’s rights independently determine internal and geopolitical interests in the digital sphere (Yarovaya, 2013). To counter American supremacy, Russia has to improve its digital sovereignty, which requires that Russia have its own ICT production, search engines, and processes along with Russian-made Internet surveillance and security systems. It also includes RUNET, which is Russia’s national segment of the Internet, and national payment systems. (Yefremov, 2017a.)

[1] For more on Russian Digital Sovereignty, see Kukkola, Ristolainen &Nikkarila, 2017

Historical, cultural and geopolitical experiences and ideology have built up the threat perception based on a sense of vulnerability. The Western powers try to maintain their positions in the world by containing "alternative centers of power," namely, Russia (UP-640, 2016). The sense of vulnerability has created a concept of Russia as a besieged fortress. To protect this besieged fortress, Russia is attempting to establish buffer zones and control neighboring spaces. The exaggeration of internal threat (Felgenhauer, 2005) caused by the KGB culture of Russian leadership (Facon, 2016) and the threat perception centered on the so-called color revolutions (Skak, 2016) have increased this perception of vulnerability. It is the Russian view that the Arab Spring was sponsored by Western intelligence services, which also attempt to influence Russian internal affairs by sponsoring political opposition. These services are increasingly using cyberspace to destabilize Russia's political and social situation. Intelligence services and terrorists are also developing malware to attack Russia's critical information infrastructure (UP-646, 2016).

According to President Putin, the Soviet Union was a besieged fortress constantly under threat of attack by the West (Aron, 2008). After the annexation of Crimea, Kremlin's besieged fortress narrative has become one of the primary means for Putin's regime to maintain power (Kolesnikov, 2016). Vladislav Surkov, the First Deputy of Russian Presidential Administration in 1999-2011 and one of the main ideologists of the Kremlin stated in 2004, that "the enemy is at the gate, and not only at the gate because in the besieged fortress there is a fifth column…sponsored by foreign states" (Ovtsarenko, 2004).

The besieged fortress concept can also be seen in Russia's cyber threat perception. Russia views itself as a besieged fortress in the information environment and in the ongoing war within the information sphere. ICT is used for military-political purposes against the sovereignty and territorial integrity of Russia. The number and severity of dangers and threats have increased in the information space. (MD, 2014.) Certain states are attacking and collecting intelligence on the Russian information infrastructure for military and political purposes (UP-646, 2016).

To counter these cyber threats, Russia is developing RUNET. The Communication Ministry's "Information Society" program aims to have 99% of RUNET traffic transferred inside Russian borders by 2020. Part of this plan is to duplicate 99% of critical RUNET infrastructure within Russia (Meduza, 2016).

One of the national interests of the RF is to maintain the stability, safety and independence of RUNET (UP-646, 2016). Because the war is waged inside Russia as well as in the information space, where a traditional military force is of little use, the role of the Federal Security Service of the Russian Federation (FSB) has increased.

A strong belief in military force has been one of the fundamental elements of Russian strategic culture. The military has had a main role in the protection of Russia and the Soviet Union. During Putin's regime the role of the security services, the Chekists, has also grown because of increased fear of internal disturbances (Facon, 2016). The FSB has been charged with surveillance of RUNET traffic with the System for Operative Investigative Activities (SORM) and the protection critical information infrastructure using GoSSOPKA, the system for detecting, preventing and eliminating the consequences of computer attacks (UP-203, 2017).

The Information Security Doctrine, published in 2000, names the backwardness of Russian ICT as a threat to the country's information security. Over the past decade, Russia has not managed to reduce the lead of Western countries in this area. In 2013, Russia was at least three to five years behind the USA in IC technology (Eliseev, 2013). This technological inferiority strengthens the Russian perception of its strategic vulnerability in the cyber environment. The use of foreign ICT challenges Russia's information security management. The insufficient level of development of Russian ICT generates a dependence on foreign technology. To improve the security of its information infrastructure, Russia had to replace imported ICT software and equipment with Russian-made counterparts and lay the foundation for technological independence in ICT production. (UP-203, 2017.)

The lack of natural borders combined with a sense of vulnerability has caused a need for a buffer zone, political and military control of neighboring spaces, and territorial expansion to natural, easily defensible borders. In the cyber environment, easily defensible borders means RUNET and digital sovereignty.

One factor that influences strategic culture is the disharmony and the clash of core principles of strategic thinking and implementation. The influence of the disharmony on Russian strategic culture was also stated in the Military Doctrine 2014. The Doctrine describes the characteristic elements of modern conflict as integrated use of military force, political, economic, and informational and other non-military measures, use of the protest potential of the population, and special operations forces and the effect on the enemy throughout the depth of its territory simultaneously in the global information space, aerospace, land and sea. The Doctrine also includes the use of irregular armed groups and private military companies, indirect and asymmetric methods and externally funded and run political forces and social movements. The concept of permanent war zone is also introduced in the Doctrine.

Gerasimov's speech in 2013 and the Military Doctrine 2014 expose the central paradigm and strategic preferences of Russian strategic culture. The Clausewitzian belief in the use of force to achieve political aims can be clearly seen, and the force is no longer exclusively military force, as it used to be. The creation of permanent war zones in the territories of parties is mentioned in the speech. Asymmetrical actions, such as the use of special operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as information operations are also part of the changed rules.

5 Conclusions

The elements of Russian strategic culture can be used to explain Russian cyber threat perception and the country's response to that threat. The central paradigm of Russian strategic culture, which includes a sense of vulnerability, the concept of the besieged fortress, a Clausewitzian belief in the use of force, and a fear of external and internal enemies and uprisings, can also be identified in the Russian view of the cyber environment. Russian strategic preferences are reflected in the cyber environment as an increased role for the security services, tightened control of RUNET, improved defense through the creation of buffer zones by RUNET, and the increasing emphasis on digital sovereignty. Disharmony and the clash of core principles of strategic thinking have influenced the Russian threat perception. The role of nonmilitary means of achieving goals has grown, the role of cyber warfare has increased, and warfare in cyberspace has become permanent.

Russian leadership feels vulnerability in the cyber environment partly for historical and geographical reasons, and partly because of the country's technical backwardness. Russia has been repeatedly attacked throughout its history, a situation that could reoccur in the cyber environment. Much like the country's physical environment, the cyber environment contains no easily defendable borders, especially because most of the ICT is made in the USA and the control of the global Internet is in American hands, which is also the main threat to Russia. That is one reason why the Kremlin is creating technical possibilities and operational preparedness to isolate RUNET from the global Internet.

The besieged fortress concept is one reason for the Russian pivot to digital sovereignty and improved protection for the critical information infrastructure of the RF. The fear of internal disturbances has increased the mandate and the responsibilities of security services in the cyber environment. The FSB has been tasked with surveilling communications in RUNET using the SORM system and to protect the critical information infrastructure of the RF with the GosSOPKA system.

REFERENCES

Almond, G & Verba, S. (1963). The Civil Culture: Political Attitudes and Democracy in Five Nations. Princeton 1963

Aron, L. (2008). The Problematic Pages. In memory of Alexander Solzhenitsyn. The New Republic. https://newrepublic.com/article/62070/the-problematic-pages

Bolden, M. & Nalla, M. (2014). Theorizing Cybercrime: Applying Routine Activities Theory. file:///C:/Users/markar/Downloads/Theorizing_Cybercrime_Applying_Routine_A.pdf

Desch, M. (1998). Culture Clash: Assessing the Importance of Ideas in Security Studies. *International Security* Vol. 23, No. 1 (Summer, 1998), pp. 141-170

Eitelhuber, N. (2009). The Russian Bear: Russian Strategic Culture and What it Implies for the West, [online], https://procon.bg/system/files/09.1.01_Eitelhuber.pdf

Ermarth, F. (2006). Russian Strategic Culture: Past, Present, and… in Transition?. Defense Threat Reduction Agency Advanced Systems and Concepts Office, [online], https://fas.org/irp/agency/dod/dtra/russia.pdf

Eliseev, I. (2013). Забил я цифрой пушку туго. Rossiyskaya Gazeta No 6085 (109), [online], https://rg.ru/2013/05/23/ashmanov.html

Facon, I. (2016). « Russian Strategic Culture in the 21st Century», [online], http://nbr.org/publications/strategic_asia/pdf/SA16_ExecutiveBrief.pdf

Felgenhauer, P. (2005). Russia's Imperial General Staff. Perspective. Volume XVI Number 1 (October- November 2005), [online], https://www.bu.edu/iscip/vol16/felgenhauer.html

Gerasimov, V. (2013). The value of science in anticipation. New challenges require rethinking the forms and methods of conducting military operations. (In Russian), [online], https://www.vpk-news.ru/articles/14632

Gray, C. (1971). What Rand Hath Wrought. Foreign Policy. No 4, Autumn 1971: 118.

Gray, C. (1999). Strategic Culture as Context: The First Generation of Theory Strikes Back. *Review of International Studies.* Vol. 25, No. 1 (Jan., 1999), pp. 49-69 Cambridge University Press

Gray, C. (2006) “Out of the Wilderness: Prime-time for Strategic Culture,” inaugural speech made at the Defense Threat Reduction Agency (DTRA) https://fas.org/irp/agency/dod/dtra/stratcult-out.pdf

Horton-Eddison, M. (2018). Is Theory of Strategic Culture Valid?, [online], https://www.academia.edu/12536463/Is_the_Theory_of_Strategic_Culture_Valid

Johnston, A. (1995a). Thinking about Strategic Culture, [online], http://www.fb03.uni-frankfurt.de/45431264/Johnston-1995-Thinking-about-Strategic-Culture.pdf

Johnston, A. (1995b). Cultural Realism: Strategic Culture and Grand Strategy in Chinese History. Princeton University Press 1995

Kolesnikov, A. (2016). Do Russians Want War? [online], http://carnegieendowment.org/files/Article_Kolesnikov_2016_Eng-2.pdf

Kukkola, J; Ristolainen, M & Nikkarila, J-P. (2017). GAME CHANGER Structural transformation of cyberspace, [online], https://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+julkaisuja+10.pdf/5d341704-816e-47be-b36d-cb1a0ccae398/PVTUTKL+julkaisuja+10.pdf.pdf

Lantis, J. (2002). Strategic Culture and National Security Policy, [online], http://www.fb03.uni-frankfurt.de/45431305/Lantis-2002--Strategic-Culture-and-National-Security-Policy.pdf

Lantis, J. (2006). "Strategic Culture and Threat Assessment”, [online], http://slideplayer.com/slide/4271931/

Lock, E. (2018) Strategic Culture Theory: What, Why, and How http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-320#acrefore-9780190228637-e-320-div1-2

MD. (2014). Military Doctrine of the RF. (in Russian), [online], https://rg.ru/2014/12/30/doktrina-dok.html

Meduza. (2016). Russia's Communications Ministry plans to isolate the RuNet by 2020. (In Russian), [online], https://meduza.io/en/news/2016/05/13/communications-ministry-plans-to-isolate-runet-by-2020

MORF. (2011). Conceptual views on the activities of the Armed Forces of the Russian Federation in the information space. (In Russian), [online], http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle#1

Murray W. (1999) "Does Military Culture Matter?", https://www.sciencedirect.com/science/article/pii/S0030438799800556?via%3Dihub

Nato (2016) Warsaw Summit Communiqué. Warsaw 8-9 July 2016 https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf

Orlov, V. (2011) Orlov on WWWW (in Russian), [online], http://www.pircenter.org/news/1196-110421-orlov-on-wwww

Ovtsarenko, Y. (2004). Vladislav Surkov, Deputy Head of the Administration of the President of the RF: Putin strengthens the State, Not Himself. (In Russian), [online], https://www.kompravda.eu/daily/23370/32473/

Putin, V. (2015). Meeting of the Valdai International Discussion Club. [online], http://en.kremlin.ru/events/president/news/50548

Snyder, J. (1977). The Soviet Strategic Culture: Implications for limited nuclear operations, [online], https://www.rand.org/content/dam/rand/pubs/reports/2005/R2154.pdf

UP-203. (2017). Strategy for the Development of an Information Society in the Russian Federation 2017-2030. (In Russian), [online], http://static.kremlin.ru/media/acts/files/0001201705100002.pdf

UP-640. (2016). Decree of the President of the RF, November 30, 2016 No. 640 "On the approval of the Foreign Policy Concept of the Russian Federation". (In Russian), [online], http://kremlin.ru/acts/bank/41451

UP-646. (2016). Decree of the President of the RF "On Approving the Doctrine of Information Security of the Russian Federation", December 5, 2016 No. 646. (In Russian), [online], http://kremlin.ru/acts/bank/41460

Zaman, R. (2009) Strategic Culture: A "Cultural" Understanding of War, Comparative Strategy, 28:1, 68-88, DOI: 10.1080/01495930802679785

Zhuang, J; Hu F. (2014).Game-Theoretic Analysis of Attack and Defense in Cyber-Physical Network Infrastructures, [online], https://www.eng.buffalo.edu/~jzhuang/Papers/HZR_ISERC2012.pdf

Yarovaya, M. (2013). Igor Ashmanov: "Today, information supremacy is like air supremacy." (In Russian), [online], https://ain.ua/2013/05/01/igor-ashmanov-segodnya-informacionnoe-dominirovanie-eto-vse-ravno-chto-gospodstvo-v-vozduxe

Yefremov, A. (2017a). Formation of the concept of information sovereignty of the state. (In Russian), [online], https://www.researchgate.net/publication/315671432_Formirovanie_koncepcii_informacionnogo_suvereniteta_gosudarstva

V

PROTECTING THE BESIEGED CYBER FORTRESS: RUSSIA'S RESPONSE TO CYBER THREATS

by

Kari, M. (2019)

Proceedings of the 18th European Conference on Cyber Warfare and Security — ECCWS 2019 (Coimbra, 2019), pp. 685–691

Protecting the Besieged Cyber Fortress: Russia’s Response to Cyber Threats

University Teacher, PhD student Martti J Kari
University of Jyväskylä
Jyväskylä Finland
martti.j.kari@jyu.fi

Abstract

The Information Security Doctrine of the Russian Federation (RF) defines the threat to information security as a complex of actions and factors that represent a danger to Russia in the information space. These threats can be information-psychological (i.e., when the adversary tries to influence a person’s mind) or information-technical (i.e., when the object of influence is the information infrastructure). The information infrastructure of the RF is a combination of information systems, websites, and communication networks located in the territory of the RF, or those used as part of international treaties signed by the RF.

A cyber threat is an illegal penetration or threat of penetration by an internal or external actor into the information infrastructure of the RF to achieve political, social, or other goals. Cyber threats against Russia are increasing and becoming more diverse. The Russian assessment of the cyber threat contains the same besieged fortress narrative as the country’s other threat assessments do. In this narrative, Russia is surrounded by hostile states and non-state actors in cyberspace. The sources of the cyber threat are Western intelligence services, terrorists, extremist movements, and criminals.

To protect itself against cyber threats, Russia is increasing its digital sovereignty by preparing to isolate the Russian segment of the Internet, RUNET, from the global Internet. Russia is also improving the protection of its critical information infrastructure. To protect itself against cyber threats but also to monitor the opposition, Russia has increased surveillance of RUNET and banned user anonymity. Russia is also making an effort to replace imported information and communication technology (ICT) with Russian production.

This paper discuss Russia’s defense against cyber threats. After the introduction, the paper begins with a description of the Russian cyber threat perception. The main section then discusses Russia’s response to this threat. This study uses grounded theory, an appropriate method for this subject because little theoretical and structured information has, to date, been published on the Russian response to cyber threats. The study data are drawn from official Russian documents such as strategies, doctrines, laws, and presidential decrees.

Keywords: Russia, cyber threat, cyber defense, cyberspace

Introduction

According to Russian authorities, the formation of cyberspace as a domain of warfare poses a threat to the Russian Federation's (RF) national interests (PP-2796, 2014) in the information space. According to the Doctrine of Information Security of the RF, Information *space* is a complex of information, objects of informatization, information systems, networks, and information technology. *Informatization* refers to social, economic, and technical processes for adopting and expanding information technology in society and throughout the country as well as to secure access to information resources. Information space includes subjects creating, generating, and processing information; subjects developing and using information technology; or subjects managing information security. It also includes mechanisms regulating the information relations in society. (UP-646, 2016.)

The threat to information security has two dimensions. First, it can be *information-psychological*, which is aimed at influencing the human mind, including its moral and intellectual world, social policy, psychological orientation, and the ability to make decisions. Second, the threat can be *information-technological*, which influences information technology systems (Kamyshev, 2009). The Russian concept of the information-technological threat corresponds to the Western concept of cyber threat. According to the Russian definition, cyberspace[1] is a limited part of the information space. Cyberspace is an environment formed by a set of communication channels on the Internet and other networks, the technological infrastructure that ensures their functioning, and any form of human activity carried out through their use. A cyber threat to Russia is an illegal penetration or threat of penetration by an internal or external actor into the information infrastructure of the RF to achieve political, social, or other goals. Cyber security is a complex of conditions under which all components of cyberspace are protected from all threats and undesirable impacts (SBRF, 2013b).

The increased interest in cyberspace as a domain of warfare has also heightened the need for theoretical studies to assess the cyber threat perceptions of different states and their responses to these threats. Although much non-academic information has been published about Russian offensive cyber capabilities and operations, only a limited amount of information has been published about the country's cyber threat scenarios and defensive cyber capabilities. However, there is enough information in official Russian legal documents to collect at least a satisfactory picture of the Russian perception of cyber threats and Russia's response to those threats. To protect itself against cyber threats, Russia is increasing its digital sovereignty by preparing to isolate the Russian segment of the Internet, RUNET, from the global Internet. Russia is also improving the protection of its critical information infrastructure. As a further means of protection against cyber threats but also as a way to monitor the opposition, Russia has increased surveillance of RUNET and banned user anonymity. In addition, Russia is making an effort to replace imported information and communication technology (ICT) with Russian production.

This paper examines Russia's defense against cyber threats. After the introduction, there is a description of the Russian cyber threat perception. The main section then discusses Russia's response to this threat. This study uses grounded theory, an appropriate method for this subject because little theoretical and structured information has, to date, been published on the Russian response to cyber threats. The study data are drawn from official Russian documents such as strategies, doctrines, laws, and presidential decrees.

Russian Cyber Threat Assessment

The National Security Strategy of the Russian Federation (UP-683, 2015) describes the world as polycentric, where the use of force in international politics is increasing. The West tries to maintain its position by containing Russia (UP-640, 2016). This confrontation between Russia and the West has extended to the information space as well

[1] киберпространство

because Western countries are using ICT against Russia to achieve their geopolitical goals (UP-683, 2015). The Kremlin sees the international arena as a battlefield, where the battle to disrupt Russia's digital sovereignty is waged every day (Sinovets, 2016). Digital sovereignty[2] means Russia's rights independently determine internal and geopolitical interests in the digital space (Yarovaya, 2013). Russian national interests – such as sovereignty, territorial integrity and constitutional order – are threatened through cyberspace by Western states, but also by terrorists and criminals. Western countries' preparations for information warfare and aspirations to change cyberspace into a war zone threaten Russia's strategic interests in the cyber environment (UP-646, 2016).

President Putin (2016) has stated that because of the risks inherent to digitalization, Russia has had to strengthen its defenses against cyber threats targeted, for example, at Russian infrastructure, the country's financial system, and the state's leadership and management. The aim of the United States is "to destroy strategic balance, to change the balance of power in such a way not just to dominate but to dictate their will to anyone" (Putin, 2015). The USA uses its technological superiority to dominate the information space (UP-646, 2016).

According to President Putin, the Soviet Union was a besieged fortress constantly under threat of attack by the West (Aron, 2008). After the annexation of Crimea, Kremlin's besieged fortress narrative has become one of the primary means for Putin's regime to maintain power (Kolesnikov, 2016). The besieged fortress view can also be seen in Russia's cyber threat perception, in which Russia describes itself as a besieged fortress in cyberspace. The number and severity of dangers and threats have increased in cyberspace, and those threats are shifting to the internal sphere of the RF (PP-2796, 2014). Vladislav Surkov, the First Deputy of Russian Presidential Administration from 1999 to 2011 and one of the main ideologists of the Kremlin, highlighted internal threats and stated in 2004 that "the enemy is at the gate, and not only at the gate because in the besieged fortress there is a fifth column…sponsored by foreign states" (Ovtsarenko, 2004).

The Military Doctrine of Russia (PP-2796, 2014) defines military danger as interstate or internal relations characterized by a combination of factors that can, under certain conditions, lead to a military threat. Such a threat can emerge in these relations when there is a real possibility of the emergence of military conflict between the opposing parties or by the high degree of readiness of a state, a coalition of states or separatist or terrorist organizations to use military force or armed violence. According to the Military Doctrine, military dangers and military threats are expanding to the information space as well as to the internal sphere of the RF. In modern conflicts, information warfare is used as a part of warfare and the enemy is impacted throughout their entire area of operation, including the global information space (PP-2796, 2014).

The Information Security Doctrine of Russia (UP-646, 2016) includes the same visions of an aggressive West discussed in the National Security Strategy and Military Doctrine. Some states are using their technological superiority to dominate the information sphere and to achieve military and political goals. An unbalanced division of responsibilities in running the Internet between the states increases this technological superiority. This prevents the safe functioning of RUNET, because actors outside Russia can block Russia's access to the Internet and destabilize the functioning of RUNET (SBRF, 2012).

The targets of cyber threats in Russian threat perception can be divided into four categories: the national interests of the RF, the information resources of the RF, the information infrastructure of the RF, and the Russian Armed Forces. The national interests of the RF are the inviolability of its constitutional order, sovereignty, independence, national and territorial integrity, and consolidating the RF's status as a leading world power (UP-640, 2016).

One of the threats to Russian national interests in cyberspace is a lack of competitive ICT and the inadequate use of information technology in the production and research and development of future technologies. This technological backwardness in ICT has created a dependence on foreign information technology. Such underdevelopment weakens Russia's cyber defenses, facilitates cyber intelligence operations in Russia, and gives Western special services an opportunity to influence Russia's information resources (UP-683, 2015; UP-646, 2016). The use of foreign ICT challenges Russia's information security management.

[2] For more on Russian Digital Sovereignty, see Kukkola, Ristolainen & Nikkarila, 2017

The Draft of the Information Security Doctrine 2015 stated that Russia is lagging behind the leading foreign states in the development of competitive information technology, including supercomputers (PUP-1, 2015). In 2013, Russia was at least three to five years behind the USA in ICT (Eliseev, 2013) and five-and-a-half years behind the USA in supercomputing technology (Moukin, 2013). This technological inferiority strengthens the Russian perception of its strategic vulnerability in cyberspace.

The exploitation of cyberspace by foreign intelligence services against Russia and the possibility of cyberspace attacks on the Russian information resource and information infrastructure have increased. Attacks against objects of its critical information infrastructure are becoming more complex, more frequent, more coordinated (UP-646, 2016), and these attacks can have a destructive impact on the infrastructure. Terrorists and extremists are among those creating means to have this kind of destructive impact (UP-203, 2017). These threats can result in a loss of control, the destruction of infrastructure, irreversible negative change (or destruction) of the economy of the country or an administrative-territorial unit or a significant, long-term deterioration in the safety of the population living in these territories (SBRF, 2012b).

Foreign special services, terrorist organizations, and extremist movements are also targeting the information infrastructure and information resources of the Russian Armed Forces (PP-2796, 2014). The main targets of possible cyberspace exploitation and attacks include strategic missile warning and defense systems, air and space defense forces, and strategic missile forces. Attackers may try to weaken the defense capability of these strategically important systems and forces (SBRF, 2013b; PP-2796, 2014). During a pre-war period and in the first phase of any hostilities, the mobilization of the Russian Armed Forces and the deployment of wartime troops to operational areas are potential targets of cyberspace attacks. The logistical systems supporting mobilization and strategic deployment would also be targets of cyberspace attacks before the outbreak of a war (SBRF, 2012; PP-2796, 2014).

Defense against Cyber Threats

The main means of Russian response to cyber threats are improved protection of the critical information infrastructure of the Russian Federation (CIIRF), a pivot to digital sovereignty by isolating RUNET from the global Internet, increased surveillance of RUNET, banning user anonymity online and the replacement of ICT imports with Russia's own ICT production.

One of Russia's national interests in the information sphere is to ensure the sustainable and uninterrupted functioning of the CIIRF (UP-646, 2016). The concept of the CIIRF was discussed already in the Russian Information Security Doctrine in 2000, hereinafter ISD 2000 (PP-1895, 2000). ISD 2000 started to debate the protection of the CIIRF, about which the core question has been the roles and responsibilities of different state authorities in information security (IS) management of the CIIRF. After ISD 2000, the protection of the CIIRF took almost two decades to organize because of the power struggle over IS management between the Federation Security Service (FSB), the Federal Service for Technical and Export Control (FSTEC), and the Russian Armed Forces, and because of the clarification of the responsibilities of private companies and other legal entities for protection.

In 2013, President Putin signed a decree on the creation of a state system for detecting, preventing, and eliminating the consequences of computer attacks on the information resources of the Russian Federation, hereinafter the GosSOPKA[3] Decree (UP-31, 2013). The GosSOPKA system is a combined, territorially distributed complex that includes authorities and means for detecting, preventing and eliminating the consequences of computer attacks on the CIIRF as well as for responding to other incidents. The GosSOPKA Decree of 2013 assigned the IS management related to cyberattacks to the FSB, but the question of the comprehensive protection of the CIIRF remained unresolved until the CII Security Law in 2017. After two drafts of a law for the security of the CIIRF, one in 2006 and the other in 2013, President Putin signed the Law on the Security of the Critical Information Infrastructure of the Russian Federation (FZ-187, 2017), hereinafter the CII Security Law, in July 2017. Its purpose is to define the CIIRF

[3] GosSOPKA is an abbreviation of the Russian phrase "state system for detecting, preventing and eliminating the consequences of computer attacks."

along with the organizational and legal basis of the IS management of the CIIRF to ensure its stable functioning when targeted by computer attacks.[4]

The critical information infrastructure of the Russian Federation (CIIRF) includes objects of critical information infrastructure as well as the telecommunication networks used to organize the interaction of these objects. The objects of the CIIRF are information systems, information and telecommunication networks, and automatic control systems operating in the following sectors: defense, healthcare, transport, communications, credit and finance, energy and fuel, nuclear, rocket and aerospace, mining, metallurgical, and chemical. The threats to the CIIRF include unauthorized access, destruction, modification, blocking, copying, provision, and dissemination of information about an object of the CIIRF (FZ-187, 2017).

In December 2017, it was confirmed that the FSB, which was tasked to create the GosSOPKA system in 2013, would also be the authority to operate GosSOPKA (UP-620, 2017). The processes implemented in the GosSOPKA framework are detecting, attributing, and responding to computer attacks; eliminating the consequences of computer attacks on the information resources of the RF; assessing the IS management situation and cyber threats; and the collection and analysis of information about computer attacks and computer incidents (SBRF, 2014; UP-620, 2017).

The FSB established and operates the National Coordination Center for Computer Incidents (NCCCI) and regional and territorial IS operations centers (SOC). The GosSOPKA SOCs will be established in the Russian Federation on the federal district[5] as well as the subject level.[6] The SOCs can be operated by the FSB, or they can be departmental or corporative SOCs. The common tasks of SOCs include collecting and analyzing information about computer attacks and computer incidents, responding to threats, and eliminating the consequences of computer incidents in information resources (UP-31, 2013).

The Federal Service for Technical and Export Control of the Russian Federation (FSTEC) is a federal executive body charged with ensuring the security of the CIIRF, countering technical intelligence, and the technical protection of information as well as a specially authorized body in the field of export control (UP-569, 2017). The identification and categorization of the objects of the CIIRF are the first steps in the process of securing and protecting it. The categorization of these objects is a process during which a subject in the CIIRF evaluates and categorizes the significance of a CII object according to the instructions of the FSTEC. Significant objects are placed into Category I, II or III. The categorization (i.e., the assigning of a category number to each object) is based on the social, political, economic, and environmental significance of the object for ensuring the country's defense, state security, and law and order. Category I is for the CIIRF's most significant objects.

After the categorization, the FSTEC specifies requirements to ensure the security of critical CIIRF objects as well as requirements to establish security systems and ensure the functioning of these objects. The FSTEC also includes requirements to ensure the security of information and telecommunications networks which are assigned to one of the three categories of significance and which, in cooperation with the Ministry of Telecom and Mass Communications of the Russian Federation, are included in the registry of significant CIIRF objects. For the banking and finance sector, the FSTEC sets requirements in consultation with the Central Bank of the Russian Federation. The subject of the CIIRF is obliged to follow FSTEC instructions and establish security arrangements corresponding to the CIIRF object's category of significance. The FSTEC is authorized to evaluate the security arrangements of the objects included in the registry (FZ-187, 2017).

The Kremlin considers digital sovereignty one of the country's main national interests in cyberspace. To secure digital sovereignty, Russia is developing RUNET, a national system of the Internet (UP-646, 2016), the functioning of which

[4] A *computer attack* is defined as the targeting of software and/or hardware in CII facilities (i.e., the telecommunication networks used to organize the interaction of such objects), with a view to violating and/or terminating their operation and/or creating a security risk that is handled by such objects information.

[5] A federal district is a grouping of the federal subjects for governing by federal governmental agencies. There are eight federal districts in Russian Federation.

[6] The subjects of the Russian Federation are the main administrative divisions in Russia.

should be stable and safe in peacetime, in the event of a direct threat of aggression, and in wartime (UP-646, 2016). This entails that it would be possible to disconnect RUNET from the global Internet (Eliseev, 2013). The Ministry of Communications' Information Society program aims to have 99% of RUNET traffic transferred inside Russian borders by 2020. Part of this plan is to duplicate 99% of RUNET's critical infrastructure within Russia (Meduza, 2016).

In December 2018, the State Duma started to discuss draft legislation to improve Russia's digital sovereignty and to ensure the sustainable operation of RUNET in the case of cyberattacks and other aggressive actions from abroad. The draft names the United States as Russia's main cyber threat and states that Russia must take measures to secure the long-term and stable functioning of RUNET and to improve the reliability of Russia's Internet resources (PZF 608767-7, 2018).

The idea of the draft is to create a Russian national system for .ru and .rf domains, and develop a Russian IP-routing system in a way that a minimum amount of Russian Internet traffic would cross the Russian border and be transferred through foreign exchange points and servers outside Russian borders. The Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) develops requirements and rules for actors that run or maintain the Internet in Russia. These actors are Internet providers, the owners of communication lines that cross Russia's national borders, the owners of technological communication networks, the owners of anonymous system numbers, and the owners of traffic exchange points (PZF 608767-7, 2018). Russian Internet providers are required to install technical equipment to counter threats to the RUNET. With this equipment, Roskomnadzor would block banned online resources in Russia and monitor compliance with the new traffic routing rules and the use of the new national domain name system. New monitoring equipment would be provided to Internet service providers (ISP) free of charge, subsidized by Roskomnadzor and the Digital Society program.

Roskomnadzor will establish a traffic-exchange registry. Service providers and companies would be forbidden from using Internet exchange points that are not on the registry. The exchange points would be banned from connecting to companies that do not comply with regulations and rules on the use of the Internet. Roskomnadzor will establish a federal agency called the Center for Monitoring and Managing Public Communication Networks. The tasks of this center are to control Internet regulations, collecting information from Russian companies about, for example, their network infrastructures, and their IP addresses, operating the internet exchange registry, and adjusting the country's traffic routing. According to the draft, the system's efficiency will be checked and improved through regular exercises, participation in which would be mandatory (PZF 608767-7, 2018).

The Russian Armed Forces have their own military intranet, which is a closed IT network specially protected against external cyberattacks. This intranet is called the Closed Data Transmission Segment (CDTS)[7] and it is not connected to the global Internet. The computers of CDTS are protected against, for example, connections by uncertified USB drives and external hard drives. The system has its own e-mail service, which allows the transfer of sensitive information, including secret and top secret documents (Tass, 2016).

Increased surveillance of RUNET is part of the RF's struggle against internal threats. The FSB has a mandate to monitor RUNET traffic. The tool for FSB Internet surveillance is the System for Operative Investigative Activities (SORM).[8] Since the 1990s, the operational capabilities of SORM systems have been improved from SORM 1 to SORM 3. SORM 1 collected mobile and fixed line telephone calls. SORM 2 began collecting Internet traffic. SORM 3 collects all kinds of communication on social networks, Wi-Fi, e-mails, Internet traffic, mobile calls, and voice-over-Internet. SORM 3 was introduced into operative use in 2014 (Soldatov and Borogan, 2015). ISPs are required to provide the FSB with statistics on all Internet traffic that passes through their servers. ISPs are also required to install SORM devices on their servers, routing all transmissions in real time through the FSB's local offices (PP-538, 2005).

[7] Закрытый сегмент передачи данны (ЗСДП)

[8] Система технических средств для обеспечения функций оперативно-розыскных мероприятий

Two laws were signed in 2017 to ban user anonymity on RUNET. Owners of virtual private network (VPN) services and Internet anonymizers are prohibited from providing access to websites banned in Russia. Roskomnadzor has authorization to block sites that provide instructions on how to circumvent government blocking (FZ-276, 2017). Companies registered in Russia as "organizers of information dissemination," including online messaging applications, are prohibited from allowing unidentified users. Those companies are required to identify their users by their cell phone numbers, and the government is tasked with elaborating the identification procedure. Mobile applications that fail to comply with requirements to restrict anonymous accounts will be blocked in Russia (FZ-241, 2017).

The information security of Russia is characterized by a lack of competitive information technology. The level of dependence of Russian industry on western ICT is high. One of the ways to correct Russia's technical backwardness in ICT and protect it against cyber threats is to develop the country's own IT sector by improving its research, development, and production of information technology (UP-646, 2016). To improve the security of its information infrastructure, Russia has to replace imported ICT software and equipment with Russian-made counterparts and lay the foundation for technological independence in ICT production (UP-203, 2017). President Putin (2018) stated that Russia needs to build its own digital platforms, ones that should be compatible with the global information space. The ISD 2000 (PP-189, 2000) had already identified the backwardness of Russian ICT as one of the main threats to the country's information security. Over the past decade, however, Russia has not managed to reduce the lead of Western countries in this area.

Conclusion

The Russian assessment of the cyber threat against it contains the same besieged fortress narrative as the country's other threat assessments do. Hostile state and non-state actors are surrounding Russia in cyberspace and cyber threats against the country are increasing and becoming more diverse. To protect itself against these cyber threats, Russia has taken operational, technical, and legal actions. The most important of these are improved protection of the CIIRF, preparations to isolate RUNET from the global Internet, intensified surveillance and the ban of user anonymity on RUNET, and the aspiration to replace imported ICT with Russian-produced ICT.

Russia is also making significant efforts to increase its digital sovereignty. It is possible that Russia will manage to create technical and operational readiness to at least partly isolate RUNET from the global Internet by the end of 2020. Russia is also improving the protection of its critical information infrastructure. The definition of the CIIRF and the division of responsibilities between authorities to protect it were confirmed by legislation in 2017 and the implementation phase has now started. The National Coordination Center for Computer Incidents (NCCCI), along with part of the regional and territorial IS operations centers, are now operational.

For Russia, the most difficult question in responding to cyber threats is that the country is lagging behind the leading foreign countries in the development of competitive information technology, including supercomputers, and this gap strengthens the Russian perception of its strategic vulnerability in cyberspace. For almost twenty years, Russia has tried, without success, to replace imported ICT software with Russian-made counterparts, and it seems that they will not succeed in the near future either. Russia is attempting to compensate for this lack mainly by isolating RUNET and by protecting the CIIRF.

REFERENCES

Eliseev I (2013) I shot digital cannon. Rossiyskaya Gazeta No 6085 (109) May 23. (in Russian) https://rg.ru/2013/05/23/ashmanov.html

FZ-187 (2017). Federation Law of the RF 187 on the Security of Critical Information Infrastructure of the Russian Federation. (in Russian), https://rg.ru/2017/07/31/bezopasnost-dok.html

FZ-241 (2017) Federal Law of the RF 241 "On Amendments to Articles 101 and 154 of the Federal Law" On Information, Information Technologies and Information Protection" (in Russian) https://rg.ru/2017/08/04/informacia-dok.html

Meduza (2016) Russia's Communications Ministry plans to isolate the RuNet by 2020. May 13, 2016. Available at: https://meduza.io/en/news/2016/05/13/communications-ministry-plans-to-isolate-runet-by-2020

PZF 608767-7 (2018) Draft of Law On Amendments to Certain Legislative Acts of the Russian Federation. (in Russian) http://www.lexfeed.ru/law/608767-7

Kamyshev, E. (2009). *Информационная безопасность и защита информации.* Information Security and Protection of Information, (in Russia), http://window.edu.ru/resource/033/75033/files/InfoBesop.pdf

Kolesnikov A (2016) Do Russians Want War?. Carnegie Moscow Center. Available at: http://carnegieendowment.org/files/Article_Kolesnikov_2016_Eng-2.pdf

Kukkola, J; Ristolainen, M & Nikkarila, J-P (2017). GAME CHANGER Structural transformation of cyberspace https://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+julkaisuja+10.pdf/5d341704-816e-47be-b36d-cb1a0ccae398/PVTUTKL+julkaisuja+10.pdf.pdf

Moukin, G. (2013). Supercomputing Gap Seen as Threat to Economy. The Moscow Times. November 28, 2013. https://themoscowtimes.com/articles/supercomputing-gap-seen-as-threat-to-economy-29999

Ovtsarenko Y (2004) Deputy Head of the Presidential Administration Vladislav Surkov: Putin is strengthening the state, not himself. (in Russian) https://www.kompravda.eu/daily/23370/32473/

PP-1895. (2000). Information Security Doctrine of the Russian Federation. http://base.garant.ru/182535/

PP-2796. (2014) Military doctrine of the Russian Federation, (in Russian), https://rg.ru/2014/12/30/doktrina-dok.html

PUP-1. (2015). Information Security Doctrine of the Russian Federation (draft). http://www.worldinwar.eu/information-security-doctrine-of-the-russian-federation-draft/

Putin, V. (2015) Meeting of the Valdai International Discussion Club. : http://en.kremlin.ru/events/president/news/50548

Putin, V. (2016) President's Speech to the Federal Assembly, (in Russian) http://kremlin.ru/events/president/news/53379

PP-538 (2005) [Decree of the Government of the Russian Federation of August 27, 2005 N 538 (ed. Of September 25, 2018) “On Approval of the Rules for Interaction of Communication Operators with Authorized State Bodies Conducting Operational-Investigation Activities. (in Russian) http://www.consultant.ru/document/cons_doc_LAW_55326/

Putin V (2018) President's Speech to the Federal Assembly]. (in Russian) http://kremlin.ru/events/president/news/56957

SBRF. (2012) The main directions of the state policy in the field of ensuring the security of automated systems for managing production and technological processes of critical infrastructure facilities of the RF, (in Russian), http://www.scrf.gov.ru/security/information/document113/

SBRF. (2013) The concept of cybersecurity strategy of the Russian Federation (Draft), (in Russian), http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

Sinovets P (2016) From Stalin to Putin: Russian Strategic Culture in the XXI Century, Its Continuity, and Change. Odessa. Mechnikov National University. http://www.davidpublisher.org/Public/uploads/Contribute/57eb1fe5a12bc.pdf

Soldatov A, Borogan I (2015) The Red Web. New York: Public Affairs

Tass (2016) In the Russian Federation developed the military Internet for the safe exchange of secret information https://tass.ru/armiya-i-opk/3715422

UP-31 (2013) Decree of the President of the Russian Federation of January 15, 2013 N 31c Moscow "On the establishment of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation" (in Russian) https://rg.ru/2013/01/18/komp-ataki-site-dok.html

UP-203. (2017) The Strategy for the Development of the Information Society in the Russian Federation for 2017-2030, (in Russian), http://www.kremlin.ru/acts/bank/41919

UP-640. (2016) Foreign Policy Concept of the Russian Federation (in Russian) http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=ru_RU

UP-646. (2016) Doctrine of Information Security of the Russian Federation, (in Russian), https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

UP-683. (2015) The National Security Strategy of the Russian Federation, (in Russian), http://pravo.gov.ru/proxy/ips/?docbody=&nd=102385609

Yarovaya M (2013) Igor Ashmanov: “Today information domination is the same as air superiority]. May 1, 2013. (in Russian) https://ain.ua/2013/05/01/igor-ashmanov-segodnya-informacionnoe-dominirovanie-eto-vse-ravno-chto-gospodstvo-v-vozduxe

VI

THEORY OF STRATEGIC CULTURE:
AN ANALYTICAL FRAMEWORK FOR RUSSIAN CYBER THREAT PERCEPTION

by

Kari, M. & Pynnöniemi, K. (2019)

Submitted to Journal of Strategic Studies.

Martti J Kari
University Teacher, Colonel (retired)
Faculty of Information Technology
University of Jyväskylä
Jyväskylä, Finland
P.O. Box 35
FI-40014 University of Jyväskylä
martti.j.kari@jyu.fi
https://www.linkedin.com/in/martti-j-kari-6a342362/
+358405076918

Katri Pynnöniemi
Assistant Professor of Russian Security Policy
National Defense University and University of Helsinki
Helsinki, Finland
Katri.pynnoniemi@helsinki.fi

THEORY OF STRATEGIC CULTURE: AN ANALYTICAL FRAMEWORK FOR RUSSIAN CYBER THREAT PERCEPTION

Abstract

The strategic environment is evolving rapidly with the recognition of cyberspace as a domain of warfare. The increased interest in cyber as a part of defense has heightened the need for theoretical tools suitable to assess cyber threat perceptions and responses to these threats. Drawing from previous research, we will formulate an analytical framework to study the formation of Russian thinking on cyber threats as a part of Russian strategic culture. This article identifies a sense of vulnerability, the narrative of Russia as a besieged fortress and the technological inferiority of Russia as specific factors influencing Russian cyber threat perception.

Keywords: Theory of strategic culture, Russia, Cyber threats, Cyberspace, Nature of the conflict

Introduction

The strategic environment is evolving rapidly with the recognition of cyber space as a domain of warfare[1]. Highlighting the threat of cyber weapons, the Russian Deputy Prime Minister Dmitry Rogozin stated in 2013 that it is possible to paralyze critical important infrastructure of an enemy state with a first strike via information networks[2]. According to Russian experts, the use of the Stuxnet malware against Iranian nuclear facilities was the first example of the new generation of warfare and showed that cyber weapons will at least partly be the ´weapon of the century´[3]. Such an attack on Russian targets could cause enormous damage to Russia's economy if the state has no counter for it[4]. Similar assessments have been voiced elsewhere. John Kerry, the US Secretary of State, stated in 2013 that cyber weapons could be considered the twenty-first century equivalent of nuclear weapons[5].

The analogy between the cyber threat and the nuclear one is based on the fact that strategic cyber weapons have revolutionized military affairs in the same way that nuclear weapons revolutionized military affairs at the end of the 1940s[6]. The use of cyber weapons against vital infrastructure may cause damage comparable to the use of nuclear weapons, although the form of the damage would be different. The increased interest in cyber as a part of defense has heightened the need for theoretical tools suitable for assessing cyber threat perceptions and responses to these threats. However, cyber security studies are a relatively new branch of study, and academic research into cyber threat perception has been limited. The existing research has concentrated on the system level and addresses, for example, cybercrime[7] or the protection of information systems against cyber attack[8].

[1] Nato, Warsaw Summit Communiqué of the North Atlantic Council in Warsaw (8-9 July 2016). https://www.nato.int/cps/en/natohq/official_texts_133169.htm and MoD, Military Doctrine of the Russian Federation (2014). https://rg.ru/2014/12/30/doktrina-dok.html

[2] Rogozin, Dmitri, Speech by Dmitry Rogozin at a press conference in the "RG" (28 June 2013). (in Russian) https://rg.ru/2013/06/28/doklad.html

[3] Orlov, Vladimir, Start of new battles, Moskovskie Novosti. (21 April 2011). (in Russian). http://www.mn.ru/newspaper/world/68636

[4] Orlov 2011

[5] Kerry, John, F, *Hearing before the Committee on Foreign Relations of United States*. (January 24, 2013) https://www.gpo.gov/fdsys/pkg/CHRG-113shrg86451/pdf/CHRG-113shrg86451.pdf

[6] Cirenza, Patrick, 'The Flawed Analogy Between Nuclear and Cyber Deterrence', *Bulletin of the Atomic Scientists* (2016 February 22). http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179

[7] See for example Jaishankar K, 2007, Establishing a Theory of Cyber Crimes. International Journal of Cyber Criminology Vol 1 Issue 2, July 2007 http://www.cybercrimejournal.com/Editoriaijccjuly.pdf; and Bolden M, Nalla M, 2014. Theorizing Cybercrime: Applying Routine Activities Theory. 2014. https://www.academia.edu/8897451/Theorizing_Cybercrime_Applying_Routine_Activities_Theory

[8] Zhuang, Rui; Bardas, Alexandru; DeLoach, Scott & Ou, Xinming, 'A Theory of Cyber Attacks A Step Towards Analyzing MTD Systems', *MTD'15 Denver CO USA* (12 October 2015). doi: 10.1145/2808475.2808478.

Given this new situation, it is important to elaborate theoretical tools for understanding strategic-level interaction in the cyber domain. This paper seeks to contribute to this effort by revitalizing theoretical approaches developed for the analysis of factors that influence strategic decision-making and, in particular, nuclear weapons policies. We argue that the theory of strategic culture is suitable for exploring and explaining the formation of Russian cyber threat perceptions and the country's subsequent cyber strategy.

This article aims to build up an analytical framework, based on the theory of strategic culture, which allows an analysis of how Russian cyber threat perceptions are formed. The following section will review the insights and shortcomings of the theory of strategic culture as it has evolved over the years. Drawing on previous research, we will formulate an analytical framework to study the formation of Russian thinking on cyber threats as a part of Russian strategic culture. One of the axioms of Russian history, according President Vladimir Putin, is that the Soviet Union has been a besieged fortress[9]. It is surrounded by potential enemies and under constant threat of attack from the West. For modern Russia, after the annexation of Crimea and the wars in eastern Ukraine and Syria, war has become a justification for the Kremlin's image of Russia as once again surrounded by enemies and under threat of attack. These events make it seem that Russia continues to view itself as a besieged fortress, so we extend this perception to the cyber realm. Based on our analysis, we argue that the Russian cyber threat assessment is based on a besieged fortress model that is similar to the one that exists in other Russian threat scenarios.

The Evolution of the Theory of Strategic Culture

The theory of strategic culture emerged from the need to understand and explain differences in the strategic thinking of the USA and the Soviet Union. The theory sought to address the problem of mirror imaging, that is, the presumption that the Soviet Union would react the way the USA does in specific conflict situations. It was also a reaction to the technological determinism[10] of security studies. Up to that point, it had been thought that nuclear weapons would make both superpowers behave similarly because the possibility of mass destruction made cultural differences irrelevant.[11]

[9] Aron, Leon, 'The Problematic Pages. In memory of Alexander Solzhenitsyn', *The New Republic*. (24 September 2008). https://newrepublic.com/article/62070/the-problematic-pages

[10] Technological determinism is a reductionist theory that aims to provide a causative link between technology and a society's nature. The theory questions the degree to which human thought or action is influenced by technological factors.

[11] Desch, Michael C, 'Culture Clash: Assessing the Importance of Ideas in Security Studies', International Security Vol. 23, No. 1 (Summer, 1998), 141-170.

Jack L. Snyder, a pioneer of this approach, suggested that organizational, political, historical and technical inputs explained differences between the strategic cultures of the two countries. He defined strategic culture as “the sum total of ideas, conditioned emotional responses, and patterns of habitual behavior that members of a national strategic community have acquired through instruction or imitation and share with each other with regard to nuclear strategy. In the area of strategy, habitual behavior is largely cognitive behavior.”[12] Snyder focused on the cognitive component of Soviet strategic culture, which he defined as “the body of attitudes and beliefs” that guides thinking on strategic questions and “influences the way strategic issues are formulated, and sets the vocabulary and conceptual parameters of strategic debate.”[13] Although the vocabulary has varied over the years, the problem formulation of strategic culture literature has remained focused on the ways in which idiosyncratic factors (history, geography, values and norms) blend with overall strategic calculations in informing and influencing decision-making on questions of peace and war.

After the initial push to integrate cultural and other idiosyncratic aspects into strategic level analysis, the theory of strategic culture has evolved in four phases and today incorporates elements from the constructivist and linguistic turn in international relations and security studies.[14] Professor Colin Gray,[15] representing the first generation, studied American strategic culture and noted that the rational-actor theories were not able to explain the proxy wars in the Middle East and the US defeat in Vietnam. This caused a need to understand why states made strategic decisions and waged war in different ways in the same kinds of situations.[16] Gray argued that the presumption that the Soviet threat perception and decision-making process are analogous to the US threat perception and decision-making might cause a dangerous illusion of safety.

The second-generation scholars started to study the relationship between strategic culture and behavior. In the early 1980s, many researchers argued that the USA was incapable of thinking and acting strategically, and the Soviet Union, as a Clausewitzian and militarily oriented

[12] Snyder J, 1977, The Soviet Strategic Culture: Implications for Limited Nuclear Operations. Santa Monica, CA: RAND Corporation, 1977, 8. https://www.rand.org/pubs/reports/R2154.html

[13] Snyder, 1977, 9

[14] Lantis, Jeffrey, S, ‘Strategic Culture and National Security Policy’, International Studies Review Vol. 4, No. 3 (Autumn, 2002), 87-113. http://www.fb03.uni-frankfurt.de/45431305/Lantis-2002--Strategic-Culture-and-National-Security-Policy.pdf and Lantis, Jeffrey, S, ‘Presentation on theme: Strategic Culture and Threat Assessment’, Second Annual Joint Threat Anticipation Center Workshop, The University of Chicago (4 April 2006). http://slideplayer.com/slide/4271931/

[15] Gray, Colin S., ‘What Rand Hath Wrought’, Foreign Policy. No 4, (Autumn 1971), 118.

[16] Gray, Colin, S., ‘Out of the Wilderness: Prime-time for Strategic Culture’, Inaugural speech made at the Defense Threat Reduction Agency (October 2006). https://fas.org/irp/agency/dod/dtra/stratcult-out.pdf

state, had an advantage in relation to the USA. Some of them considered the USA weak and unable to challenge the authoritarian Soviet Union. These forecasts proved wrong because researchers were not able to understand the internal and political changes in the Soviet Union well enough to predict its collapse at the beginning of the 1990s. This failure led to a new approach to strategic culture studies.[17]

In the early 1990s, constructivism became one of the major schools in the study of international relations. In contrast to neorealism and neoliberalism, constructivism stressed that historical and social constructions are the basics of international relations. At the same time, strategic culture studies expanded beyond nuclear war, and were inspired by constructivism. One of the representatives of this third generation is Alastair Iain Johnston. His book *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*[18] is considered a basic work of this new approach.[19] Johnston studied the character and linkages of Chinese strategic culture to the use of military force against external threats. Johnston defines strategic culture as the following:

> ‘an integrated system of symbols (e.g. argumentation, structures, languages, analogies, metaphors) which acts to establish pervasive and long-lasting grand strategic preferences by formulating concepts of the role and efficacy of military force in interstate political affairs, and by clothing these conceptions with such an aura of factuality that the strategic preferences seem uniquely realistic and efficacious*’*.[20]

The fourth-generation of strategic culture, based on constructivist ideas, followed Snyder’s definition of strategic culture as “a set of elite beliefs, attitudes, and behavior patterns socialized into a distinctive mode of thought.”[21] Moreover, later research has shared Snyder’s view that multiple subcultures could exist inside a strategic culture and that competition among subcultures creates a number of strategic options.[22] Different subcultures influence strategic culture, and by following and understanding the argumentation between different groups (i.e., between

[17] Desch 1998

[18] Johnston, Alistair, Cultural Realism: Strategic Culture and Grand Strategy in Chinese History. (New Jersey: Princeton University Press 1995b)

[19] Lantis 2006

[20] Johnston, Alistair, ‘Thinking about Strategic Culture’, International Security Vol. 19, No. 4 (Spring, 1995a), 32-64. http://www.fb03.uni-frankfurt.de/45431264/Johnston-1995-Thinking-about-Strategic-Culture.pdf

[21] Lantis 2002

[22] Howlett D & Glenn J, Nordic strategic culture. Cooperation and conflict, 40 (1) (2005), 121–140. doi: 10.1177/0010836705049737; Lantis 2002

or within organizations) it might be possible to predict changes in a state's strategic culture.[23] Identifying the content of ideas of competing subcultures might be possible to describe how strategic culture influences policy change.[24]

However, much of the literature on strategic culture takes a critical view on the theory's predictive power. Writing in the mid-1990s, Johnston argued that the theory has been "unable to offer a convincing research design for isolating the effects of strategic culture."[25] In other words, the theory has been unable to explain why decision-makers have made certain choices rather than others. Instead, previous versions of the theory have assumed, implicitly or explicitly, that different policy choices stem from a historically and culturally embedded, and therefore unique, understanding of the strategic calculus in a specific context.[26] When in fact, the opposite may be the case, namely that the strategic culture is not unique to a particular state but similar features of strategic thinking are shared by groups of states along the *realpolitik* versus *idealpolitik* continuum.[27]

Despite being critical of the work of previous generations, Johnston has sought to develop this theory further. He argued that only with "the careful analysis of strategic culture could policymakers establish more accurate and emphatic understandings of how different actors perceive the game being played, reducing uncertainty and other information problems in strategic choice. "Yet bad analysis," in Johnston's words, could lead in the opposite direction, reinforcing "stereotypes about the strategic predispositions of other states and close off policy alternatives deemed inappropriate for dealing with the local strategic cultures."[28]

As formulated in one of the recent works on this topic, the task is to "understand rationality within a cultural context,"[29] and consequently, provide more accurate understanding of what deterrence is and how it works in different cultural and political contexts. Consequently, simplistic assumptions of the relationship between culture and strategic decision-making have been refuted. As one of the theorists of the first generation, Colin Gray, has said, "strategic

[23] Bloomfeld, Alan, 'Time to Move On: Reconceptualizing the Strategic Culture Debate.' Contemporary Security Policy 33(3) (Dec 2012) 437-461. doi: 10.1080/13523260.2012.727679; Davis Cross, Mai´a K, 'Rethinking epistemic communities twenty years later', Review of International Studies Vol 39, Issue 1 (Jan 2013), 137-160. doi: 10.1017/S0260210512000034

[24] Libel, Tamir, 'Explaining the security paradigm shift: strategic culture, epistemic communities, and Israel's changing national security policy', Defence Studies (March 2016), 137-156. doi: 10.1080/14702436.2016.1165595

[25] Johnston 1995a

[26] Johnston, 1995a: 33

[27] Johnston, 1995a: 60

[28] Johnston, 1995a: 64

[29] Johnson, Jeannie L, 'Conclusion: toward a standard methodological approach', in Johnson, Jeannie L., Kerry M. Kartchner, and Jeffrey A. Larsen, *Strategic culture and weapons of mass destruction. Culturally based insights into comparative national security policymaking*. (NY: Palgrave Macmillan 2009).

culture should be approached both as a shaping context for behavior and itself as a constituent of that behavior."[30] Gray has later continued to advocate a parsimonious approach to methodology and theory, keeping the focus on the "plot," that is, the ways in which "cultural assumptions" are adopted, accepted and digested and thereby condition the strategic decision-making.[31]

The above discussion makes it clear that strategic culture theory has developed from its original 1970s form as the scholarly attention has shifted from behaviorism towards constructivism, yet the main questions remain remarkably similar. The body of research on strategic culture has not provided a one-size-fits-all conceptualization of strategic culture or defined its explanatory power in simple terms.[32] The work in this area continues, as exemplified by the promising concept of "cultural topography,"[33] whereas others[34] continue to prefer a less rigorous approach to analysis.

Despite these shortcomings in theory building and the fact that Johnston's analytical framework is almost 25 years old, it has been selected as an analytical framework for this paper. Johnston's construction of strategic culture remains valid and provides good insight and a suitable framework to explain the cause of behavior, in this case, Russian cyber threat perception and response to cyber threats. The main advantage of this version of the strategic culture theory is in how it defines and describes components of a strategic culture (i.e., its central paradigm and strategic preferences), both of which are easier to identify and describe than unstructured state behavior. Another advantage is that strategic culture considers state-specific factors, which influence state behavior. One disadvantage is that among scholars there is no common view of what the independent and dependent variables of strategic culture are. Even though strategic culture can be criticized[35] as a vaguely defined concept with logical inconsistencies, it can also

[30] Gray 1999, 50

[31] Cray, Colin S, 'Out of the wilderness: prime time for strategic culture', in Johnson, Jeannie L., Kerry M. Kartchner, and Jeffrey A. Larsen, *Strategic culture and weapons of mass destruction. Culturally based insights into comparative national security policymaking*. (NY: Palgrave Macmillan 2009).

32 Horton-Eddison, Martin, 'Is Theory of Strategic Culture Valid?' (2018). https://www.academia.edu/12536463/Is_the_Theory_of_Strategic_Culture_Valid

33 Berrett, Matthew T and Johnson, Jeannie L, 'Cultural Topography: A New Research Tool for Intelligence Analysis — Central Intelligence Agency.', Studies in Intelligence Vol. 55, No. 2 (June 2011). https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-2/pdfs-vol.-55-no.-2/Berrett-Cultural%20Topography-9June2011.pdf see also Johnson, Jeannie L 2009. 'Conclusion: toward a standard methodological approach', in Johnson, Jeannie L., Kerry M. Kartchner, and Jeffrey A. Larsen 2009. Strategic culture and weapons of mass destruction. Culturally based insights into comparative national security policymaking. NY: Palgrave Macmillan.

34 Cray 2006

35 see Horton-Eddison 2018; Lock, E. 2018. Strategic Culture Theory: What, Why, and How. doi: 10.1093/acrefore/9780190228637.013.320; See debate Echevarria II, Antulio J and Hoffman, Frank, 'Review Essay - Strategic Culture And Ways Of War, Elusive Fiction Or Essential Concept?', Naval War College Review: Vol. 70 : No. 2 , Article 7 (2017). https://digital-commons.usnwc.edu/nwc-review/vol70/iss2/7/

be used as a tool for providing framework and context for developments in a specific policy field (here the field being cyber).

This paper follows Johnston's idea about the separation of strategic culture, that is, its central paradigm and strategic preferences from state behavior in practice. Russian state behavior in the cyber environment in practice is difficult to explore, but the central paradigm and strategic preferences can be identified through the analysis of Russian official documentation. The central paradigm can be found in strategic level documents as strategies and doctrines and this applies in cyberspace. State behavior in practice is difficult to monitor but strategic preferences can be identified in lower-level documentation as laws and guidance documents of state agencies and ministries.

Historical and geographical factors, such as several invasions of Russia or the country's lack of defensible borders have influenced the central paradigm of Russian strategic culture. In other words, these factors have, along with the central paradigm, influenced Russia's strategic preferences to respond to threats. This applies in cyberspace as well.

The essence of the central paradigm of Russian strategic culture is a sense of vulnerability that translates into a concept of permanent war. This derives from geography, namely, the lack of defensible borders coupled with the historical experience of foreign invasions to Russia. Together, these factors are amalgamated in the Russian general threat perception based on the narrative of besieged fortress.[36] It also applies in cyberspace. The main purpose of this paper is to explain the formation of Russian thinking on cyber threats as a part of Russian strategic culture and, as Stuart Moore proposes, "generate more empirical research into particular strategic cultural cases through the use of thick description."[37]

An Analytical Framework for Studying the Perception of Cyber Threats

Central Paradigm and Strategic Preferences of Strategic Culture

´The strategic culture,´ argues Johnston, ´if it exists, is an ideational milieu, which limits behavioral choices´[38]. Johnston proposes a definition of strategic culture as a ´system of symbols´

[36] Adamsky, Dima, 'Cultural Underpinnings of Current Russian Nuclear and Security Strategy', in J.L. Johnson, Kerry Kartchner and Marilyn Maines (eds) Crossing Nuclear Thresholds. Leveraging Sociocultural Insights into Nuclear Decisionmaking. (NY: Palgrave Macmillan 2018)

[37] Poore, Stuart, 'What is the context? A reply to the Gray-Johnston debate on strategic culture', Review of International Studies 29 (2003), 279-284. DOI: 10.1017/S0260210503000172

[38] Johnston, 1995a: 46

that has two parts. The first part is the central paradigm of strategic culture[39]. This consists of general assumptions ´about the orderliness of the strategic environment,´ including the following[40]:

- the role of war in human affairs (whether it is inevitable or an aberration)
- the nature of the adversary and the threat it poses (zero-sum or variable sum)
- the efficacy of the use of force (about the ability to control outcomes and to eliminate threats, and the conditions under which applied force is useful).

The second part in Johnston's system consists of assumptions at a more operational level about what strategic options are the most efficacious for dealing with the threat environment as defined by the answers to the first three variables mentioned above[41]. Accordingly, understanding the strategic culture of another country is vital because it helps to understand its strategic policy variables and the underlying threat assessments and situational awareness in specific (conflict) situations[42].

Different states have different patterns of action and strategic preferences, which are solidified in historical experiences related especially to the threat and use of force. Strategic preferences are influenced by the philosophical, political, cultural, and cognitive experiences of decision-makers. However, there is not always a clear causal relationship between symbolic strategic discourse and operational strategy. Studies in psychology, anthropology and linguistics have broadly shown that symbols can be used for three purposes, each with differing effects on strategic choice. The first purpose is so-called auto communication, which means that the strategies are not meant to be implemented. They are linguistic means to strengthen the sense of competence and legitimacy of elites and decision-makers. One example of a discourse not meant to be implemented is the deterrence theory. Declaratory nuclear doctrine differs from operational doctrine. Auto communication symbols, myths and strategies do not have an effect on the strategic behavior of a state.[43]

The second purpose of symbols is that elites can use them in official language directed at other members in the community. By using official language, elites can exclude alternative

[39] Johnston, 1995b: ix–x, 248
[40] Johnston, 1995a: 46
[41] Johnston, 1995a, 46
[42] Booth K, 2005, Strategic Culture: Validity and Validation. *Oxford Journal on Good Governance*. Volume 2 – Number 1 March 2005. pp. 25-28. http://ocgg.org/fileadmin/Journal/OJGG_Vol_2_No_1.pdf and Gray 2006
[43] Johnston, 1995a: 57

strategies and other actions that might challenge their authority. Official language is also used to maintain and increase the support of elites. Others normally recognize the users of official language as legitimate and competent authorities, which means that they also accept the decisions even though there might be severe consequences. Political leadership, the military and the defense industry have their own interest to limit strategic discourse and those who want to join the debate had to adapt their language to the official discourse in order to gain acceptance. Official language and symbols constrain behavior in a measurable way.[44]

The third purpose of using symbols is to create and increase solidarity inside the so-called political community. The political community is a community, bound together with myths and language that highlight the uniqueness of the community. The solidarity, which bounds the group together, is typically directed at others, at possible adversaries. Myths are used to describe one's own community and its values as well as to dehumanize the adversary.

Johnston's work has been criticized, especially because he separates strategic culture from behavior. One of Johnston's critics, Colin Gray,[45] stated that strategic behavior cannot be isolated from strategic culture, and that it is more important to understand strategic behavior than it is to explain it. Therefore, the theory of strategic culture should try to interpret the meaning of strategic behavior rather than explain the cause of that behavior. Johnston, however, views strategic culture as an independent and isolatable variable, which causes the behavioral choices of states. In Johnston's model, causality moves from culture to behavior.

This article follows Johnston's idea about the disjunction of strategic culture from state behavior. State behavior is difficult, and in some cases even impossible, to detect, observe, and measure. Johnston's definition of strategic culture and his division of strategic culture into the two main components of a central paradigm and strategic preferences form a framework for the discussion in this study. Here we explain what factors influence Russian strategic culture and how they influence it. Then follows a discussion of the central paradigm and strategic preferences on a general level and then Russia's strategic preferences in cyberspace are examined.

The fundamental elements of a strategic culture reflect its central paradigm, that is, its assumptions about the nature and role of conflict and the enemy, about the threat posed by the enemy, and about the efficacy of the use of force against these threats. Strategic preferences, that is, assumptions about how to deal with threats, can be derived from this central paradigm. Johnston[46] sees that one productive way to identify a central paradigm and strategic preferences

[44] Johnston, 1995a: 55
[45] Gray 1999
[46] Johnston 1995b

is to analyze the content of recent texts related to the subject in question. The central paradigm of Russian strategic culture can be observed in subject-related high-level documents, such as strategies and doctrines. Strategic preferences, derived from the central paradigm and from the high-level documents, can be found in doctrines and more practical level documents such as laws and guidance documents of different security-related state organizations.

Research Data on Russian Strategic Culture

As Snyder[47] stated in the 1970s, every government needs to carry out professional military inquires and policy formulation. Snyder established the validity of Soviet open source data by comparing the topics in Russian open source publications and restricted ones. By placing the raw data into a coherent political or organizational context, it was possible to understand the ideas behind official Soviet statements and actions. The same idea is applied here in the study of Russia's cyber threat picture and cyber security management.

Russian strategies and doctrines on security policy aim to inform other parties, namely foreign countries, about Russian policy formulation. These documents also provide normative and legislative guidance to Russian authorities and society on protection against security threats in the cyber domain. This means that even if the amount of information published about real Russian cyber threat scenarios is limited, there is enough information scattered in official documents to build up at least a satisfactory description of the country's perception of cyber threats.

According to the law on strategic planning of the Russian Federation[48], the hierarchy of Russian official documents for strategic planning in the area of cyber threat perception and cyber security management includes the following documents:

- Annual speech of the president to the Federal Assembly
- Strategy for the Development of an Information Society in the RF 2017-2030
- National security strategy
- Main directions and bases of policies
- Doctrines
- Other records and documents

[47] Snyder 1977

[48] FZ-172 (2014) Federal Law 172 of 28 June 2014 on Strategic Planning in the Russian Federation. https://rg.ru/2014/07/03/strategia-dok.html

The Russian Federation President’s annual address to the Federal Assembly, the upper chamber of Russian parliament, is one the guidelines for strategic planning in Russia[49]. President Putin has mentioned the cyber threat and cyber security management only a few times. In December 2016, Putin[50] stated that because of the risks included in digital technologies, Russia must strengthen its defenses against cyber threats and make all the elements of its infrastructure, financial system, and state leadership and management more stable. Later, in his 1 March 2018 address Putin stated the following:

> ´We are greatly concerned by certain provisions of the revised nuclear posture review, which expand the opportunities to reduce the threshold for the use of nuclear arms. Behind closed doors, one may say anything to calm down anyone, but we read what is written. And what is written is that this strategy can be put into action in response to conventional arms attacks and even to a cyber threat.´ [51]

The Strategy for the Development of an Information Society in the Russian Federation 2017-2030[52] defines the aims, tasks and means of implementation of foreign and internal policy of Russia related to the use of information and communication technology to develop an information society, create a national digital economy, and support national interests and strategic national priorities.

The National Security Strategy[53] is the basic strategic planning document defining the national interests of Russia and its strategic national priorities, objectives, tasks, and measures in domestic and foreign policy aimed at strengthening the national security of Russia and ensuring the country’s sustainable development in the long term. The National Security Strategy defines the national security of Russia as the protection of the individual, society, and the state against internal and external threats. National security includes defense of the country and all

[49] FZ-172 (2014)

[50] Putin, Vladimir, President's Speech to the Federal Assembly (1 December 2016). (in Russian) http://kremlin.ru/events/president/news/53379

[51] Putin, Vladimir, President's Speech to the Federal Assembly (1 March 2018). (in Russian) http://kremlin.ru/events/president/news/56957

[52] UP-203 (2017) Decree 203 of the President of the RF of 9 May 2017 On the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030. (in Russian) http://kremlin.ru/acts/bank/41919

[53] UP- 683 (2015) Decree 683 of the President of the RF of 31 December 2015 About the National Security Strategy of the Russian Federation. (in Russian) http://pravo.gov.ru/proxy/ips/?docbody=&nd=102385609

types of security envisioned by the Constitution and legislation of Russia—primarily state, public, informational, environmental, economic, and transportation as well as energy security and individual security. [54]

The Foreign Policy Concept of the Russian Federation approved in November 2016 is a collection of the basic principles, priority areas, goals and objectives of the foreign policy of the Russian Federation. The concept provides a systemic vision of the basic principles, priority areas, goals and objectives of Russia's foreign policy. The aims of the Foreign Policy Concept 2016 are to ensure national security, sovereignty, and territorial integrity and to consolidate Russia's position as a center of influence in today's world.

According to the concept, Russia will take the necessary measures to ensure national and international cyber security and counter threats to the state emanating from cyberspace. Russia will also combat terrorism and other criminal threats involving the use of information and communication technology and deter the use of ICT for military-political aims that run counter to international law, including actions aimed at interfering in the domestic affairs of states. Under the auspices of the UN, Russia seeks to devise universal rules of responsible behavior for international cyber security, including by rendering Internet governance to be more international in a fair manner. [55]

From the point of view of Russia's cyber threat perception, the most important subject-related doctrines are the Military Doctrine of Russia[56] and the Information Security Doctrine of Russia[57]. The Military Doctrine 2014 reflects the central paradigm of Russian strategic culture. It is a collection of official views on the nature and role of conflict and the threat posed to Russia and on the use of force against these threats. The Military Doctrine 2014 establishes a framework for the Information Security Doctrine, both of which discuss the paradigm and strategic preferences in the cyber environment.

The Information Security Doctrine 2016 constitutes a system of official views on ensuring the national security of the Russian Federation in the information sphere. The IS Doctrine discusses both paradigm and strategic preferences of Russian strategic culture in the cyber environment. The IS Doctrine's paradigm includes descriptions of the information environment, the

[54] UP-683 (2015)

[55] MFA, Foreign Policy Concept of the Russian Federation (30 November 2016.) http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248

[56] MoD 2014

[57] UP-646 (2016) Doctrine of Information Security of the RF. (in Russian) https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

national interests of Russia and threats to Russia in the information environment. The strategic preferences of IS management and its main directions are discussed in the doctrine.[58]

The IS Doctrine defines the information sphere as a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet. It also includes communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security. In addition, there is a set of mechanisms regulating public relations in the sphere.[59]

Other records and documents dealing with cyber threat perception and cyber security management include subject-related laws, decrees, executive orders and other legislative documents and normative and methodological documents[60]. The subject-related laws and other legislative documents include the following:

- International information security agreements signed by the Russian Federation
- Constitution of the Russian Federation
- Legislation of the Russian Federation
- Decrees (*Ukaz*, 'executive order') of the President of the Russian Federation
- Decisions and orders of the Russian Federation Government

A Decree of the President of the Russian Federation, as a normative legal act, has the status of a by-law in the hierarchy of legal acts. A by-law is a rule or law established by an organization or community to regulate itself, as allowed or provided for by some higher authority. The Government of Russia can issue decisions and orders. Presidential decrees and governmental decisions and orders may not alter existing laws of higher precedence. Normative and methodological documents discussing cyber threat perception and cyber security management include the following:

- Documents of the Security Council of Russia
- Documents of the Federation Security Service (FSB)

58 UP-646 (2016)

[59] UP-646 (2016)

[60] Lapina M, Revin A & Lapin V, Информационное право [Information Law] (Moscow: Zakon i pravo 2004) and Komarov, Aleksei, 'Normative documents on the safety of automated control systems and critical information infrastructure' (21 July 2016). (in Russian) http://www.securitylab.ru/blog/personal/zlonov/144489.php

- Documents of the Russian Technical and Export Controls Federation Service (FSTEC)
- Legal norms of the Russian Federation Ministries and Administrations
- State Standards of the Russian Federation

The Security Council of Russia drafts policy proposals on defending the interests of Russia against internal and external threats. The council helps determine security policy of the Russian Federation. Agencies such as the Federation Security Service (FSB) and the Federal Service for Technical and Export Control (FSTEC) may enact regulations through their general competency[61]. These documents, usually orders and instructions, are limited to the extent of the constitution and relevant codes.

Russian Strategic Thinking on Cyber Threats

Nature of the conflict

A conception about the nature of the conflict is a part of the central paradigm of strategic culture. The main strategic documents emphasize the view of the Kremlin that the international scene is polycentric, dangerous, chaotic, and volatile[62]. The Foreign Policy Concept 2016 highlights that Western powers are attempting to maintain their positions in the world by containing ´alternative centers of power,´ including Russia. This containment policy leads to international instability and turbulence[63]. The same idea is expressed already in the National Security Strategy[64], where it is stated that the US and its allies oppose the rise of Russian influence in global politics. Wars in the former Yugoslavia in the 1990s, the color revolutions in the Arab countries and near Russia in Georgia and Ukraine have strengthened the impression that the major threat to Russia comes from the West[65]. This is exemplified by accusations that the support of the USA and the EU for the anti-constitutional coup d'état in Ukraine led to an armed conflict[66].

[61] UP-569 (2017) Decree 569 of the President of the RF of 25 November 2017 on Amendments to the Regulations on the Federal Service for Technical and Export Control. (in Russian) http://kremlin.ru/acts/bank/42489
[62] See for example MoD 2014, UP-683 (2015); and MFA 2016
[63] MFA 2016
[64] UP-683 (2015)
[65] Facon, Isabella, 'Russian Strategic Culture in the 21st Century: Redefining the West-East Balance', in Tellis A, Szalwinski A and Wills M (eds) *Understanding Strategic Cultures in the Asia-Pacific*, *Strategic Asia 2016-2017*, The National Bureau of Asian Research, (2016) 62-89. http://nbr.org/publications/strategic_asia/pdf/SA16_ExecutiveBrief.pdf
[66] UP-683 (2015)

Although the role of the EU is highlighted in some of the documents, the USA remains Russia's main rival and an ′evil′ that tries to undermine Russia's status as a great power. From the Russian point of view, NATO expansion has destroyed the balance of power and the buffer zones the country has enjoyed with the West[67].

The strategic-level documents describe the current situation in the world in terms of increased competition for natural and human resources. The emphasis on continuing struggle or competition between the major powers is a characteristic feature of official rhetoric[68]. The Military Doctrine 2014 argues that many regional conflicts are unresolved and there is a tendency to use force for their resolution, including in the regions bordering on the Russian Federation. Although the probability of large-scale war against the Russian Federation has diminished, military dangers for the Russian Federation have grown. Military dangers also affect the internal situation of the country[69].

One factor that influences the formulation of strategic culture is the disharmony and clash of core principles in strategic thinking and implementation. A disharmony that is influencing Russian strategic culture was exposed in a speech published in February 2013 by General Valeri Gerasimov, the Chief of the Russian General Staff. Gerasimov stated that the nature and rules of war have changed. According to Gerasimov, the role of non-military means in achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of weapons in their effectiveness. The lines between war and peace have been blurred, wars are no longer declared, and after they have begun, they proceed according to an unfamiliar template.[70]

These changed rules of warfare were also stated in the Military Doctrine 2014. The elements of modern conflict are the integrated use of military force with political, economic, informational and other non-military measures, use of the protest potential of the population, and special operations forces and affecting the enemy throughout the depth of its territory in the global information space, aerospace, land and sea. Modern conflict also typically utilizes pri-

[67] Sinovets, Polina, 'From Stalin to Putin: Russian Strategic Culture in the XXI Century, Its Continuity, and Change', *Philosophy Study* Vol. 6, No. 7 (July 2016), 417-423 doi: 10.17265/2159-5313/2016.07.002

[68] Pynnöniemi, Katri, 'Russia's National Security Strategy: Analysis of Conceptual Evolution', *The Journal of Slavic Military Studies* 31:2 (2018) 240-256.

[69] MoD 2014

[70] Gerasimov, Valeri, 'The value of science in anticipation. New challenges require rethinking the forms and methods of conducting military operations', *Voenno-Promyshlennyi Kurier* (26 February 2013). (in Russian) https://www.vpk-news.ru/articles/14632

vate military companies, indirect and asymmetric methods, and externally funded and run political forces and social movements. A further characteristic of modern military conflicts is the creation of permanent warfare zones in the territories of the opposing sides[71].

In recent years, beginning with the occupation of Crimea in 2014, the Kremlin has created a concept of permanent war by telling the Russian people that Russia is under siege. As a besieged fortress, the logic suggests, the country needs to be protected and its external aggression is part of a defensive war or actually part of a series of simple, low-cost military operations. Putin has even explicitly stated that the Soviet Union is a besieged fortress constantly under threat of attack by the West[72]. The American diplomat George Kennan has explained that using the concept of a besieged fortress was one way for the Soviet authorities to maintain their authority.[73] This might be one reason for the use of the same narrative by the Kremlin's present leadership. According to this narrative, also known as the enemy-at-the-gate narrative, as used by Dmitri Peshkov, spokesperson for President Putin, in 2004[74], there is the continuous threat of an attack by the West. This threat legitimizes the Kremlin's authoritarian rule, a centralized command and control system, and the broad mandate of the Russian security services[75].

The perception that Russia's resources and territory are targets of bellicose enemy states[76] and the country's perceived geostrategic and technological vulnerability[77], combined with Russia's feeling of a hostile world [78], have strengthened the Russian logic of the besieged fortress[79]. To protect this fortress, Russia attempts to maintain its influence in post-Soviet space by estab-

[71] MoD 2014

[72] Aron 2008

[73] Kennan, George, 'The Sources of Soviet Conduct', *Foreign Affairs* 25 (1947), 566-82. https://is.muni.cz/el/1423/jaro2017/BSS185/um/Week_4_Kennan_on_Containment.pdf

[74] Monaghan, Andrew, ''An enemy at the gates' or 'from victory to victory'?', *Russian foreign policy. International Affairs* 84(4) (2008), 717-733. http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2346.2008.00734.x/abstract

[75] Kolesnikov, Andrei, 'Do Russians Want War?', *Carnegie Moscow Center* (June 2016). http://carnegieendowment.org/files/Article_Kolesnikov_2016_Eng-2.pdf

[76] Facon 2016

[77] Covington, Stephen R. 'The Culture of Strategic Thought Behind Russia's Modern Approaches to Warfare.' Belfer Center. Harvard Kennedy School. (2016). https://www.belfercenter.org/sites/default/files/files/publication/Culture%20of%20Strategic%20Thought%203.pdf

[78] Facon, Isabella, 'Russia's national security strategy and military doctrine and their implications for the EU', *European Parliament's Sub-Committee on Security and Defence* (2017). http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/578016/EXPO_IDA(2017)578016_EN.pdf

[79] Igumnova Lyudmila, 'Russia's Strategic Culture Between American and European Worldviews', *The Journal of Slavic Military Studies,* Volume 24 (2011). doi: 10.1080/13518046.2011.572729

lishing buffer zones and controlling neighboring areas. The exaggeration of external and internal threats[80], which stems from the KGB culture of Russian leadership[81] and the Chekist threat perception centered on color revolutions[82], have influenced this perception of vulnerability.

The conflict has expanded to cyberspace. According to Igor Ashmanov, a Russian ICT specialist, the cyber struggle against the digital sovereignty of Russia is waged every day and no rules of war apply to it[83]. In Russian terms, digital sovereignty refers to the rights of the state and its possibilities to independently determine national internal and geopolitical interests in the digital sphere. Digital sovereignty includes opportunities to implement the state's own information policy and organize information resources and the infrastructure of information space to ensure the state's digital security against the threat posed by the enemy.

According to the IS Doctrine 2016, a number of foreign countries are building up their information technology capacities to influence the information infrastructure of Russia in pursuing military and political purposes. Certain states use their technological superiority to dominate cyberspace. The concepts of the besieged fortress and permanent war are also stated in the IS Doctrine 2016. Certain states and organizations are attacking in the cyber environment and collecting intelligence on the information infrastructure of Russia for military and political purposes.[84]

As a part of this permanent war, one of the national interests of Russia in the information sphere is to maintain the safe and stable functioning as well as the independence of the Russian segment of the Internet, RUNET. This primarily concerns the critical information infrastructure and the integrated telecommunications network of the Russian Federation.

Most ICT, especially software, is made in the US, and US-led companies and organizations control the Internet. According to the IS Doctrine 2016, this current global distribution of resources makes it impossible to manage the Internet jointly in a fair and trust-based manner. The absence of international legal norms regulating interstate relations in the information space makes it difficult to create an international information security system and to achieve strategic stability and an equitable strategic partnership in information space[85].

[80] Felgenhauer, Pavel, 'Russia's Imperial General Staff', *Perspective.* Volume XVI Number 1 (October- November 2005). https://www.bu.edu/iscip/vol16/felgenhauer.html

[81] Facon 2016

[82] Skak, Mette, 'Russian strategic culture: the role of today's chekisty', *Contemporary Politics*. Vol. 22, Iss. 3 (2016), 324-341. doi: 10.1080/13569775.2016.1201317

[83] Yarovaya, M, 'Igor Ashmanov: 'Today information domination is the same as air superiority'', (1 May 2013). (in Russian) https://ain.ua/2013/05/01/igor-ashmanov-segodnya-informacionnoe-dominirovanie-eto-vse-ravno-chto-gospodstvo-v-vozduxe

[84] UP-646 (2016)

[85] UP-646 (2016)

Threat posed by the enemy

In addition to a conception about the nature of a conflict, the central paradigm of any strategic culture also includes a conception about the nature of the adversary and the threat it poses[86]. The Military Doctrine 2014 divides an adversary's possible activities against Russia into two components—danger and threat—both of which can be external and internal. A military danger is a state of interstate or domestic relations characterized by a set of factors that could, under certain conditions, lead to a military threat. A military threat is a state of interstate or domestic relations characterized by the possibility of a military conflict between the opposing sides.

The Military Doctrine 2014 names NATO as one of Russia's main external military dangers. NATO's potential and actual violations of international law, as well as the approach of NATO's military infrastructure to Russian borders, are defined as military dangers. External military dangers also include the deployment of foreign military contingents or strategic missile defense systems near the borders of Russia as external military dangers. Territorial claims against the Russian Federation and its allies and interference in their internal affairs are considered military dangers. So too are the establishment of regimes or the implementation of policies that threaten the interests of Russia, the overthrowing of legitimate leadership in neighboring states, and the subversive operations of foreign special services and their coalitions against Russia.

The use of information and communication technologies for military-political purposes aimed against the sovereignty, political independence, and territorial integrity of Russia is mentioned as a military danger in information and cyberspace. Another cyber-related military threat to Russia is the obstruction of the functioning of the state and military command and control systems. This includes the disruption of the functioning of strategic nuclear forces, missile attack warning systems, space control, and nuclear munitions storage facilities as well as of hazardous facilities such as those in the nuclear, chemical, pharmaceutical, medical and other industries.

Internal military dangers include efforts to change the constitutional system, destabilize the political and social situation, or disrupt the functioning of governmental or military bodies or the information infrastructure of the RF. The informational impact on the population, pro-

[86] Johnston 1995a: 46

voking interethnic and social tension, and extremism are also defined as internal military dangers. Especially threats in cyberspace are often non-military in character. According to the IS Doctrine 2016, threats to the information security of Russia include internal and external actions and factors creating a risk to the national interests of Russia in the information sphere.[87] Factors creating a risk can be information technical, when information technology systems are targets of influence in cyber space, or information psychological, when the adversary tries to influence a person's mind, their moral and mental world, social-political opinions and ability to make decisions[88]. Cyberspace consists of a technological infrastructure that enables the functionality of the Internet and other telecommunication networks, as well as of all human activity implemented on the Internet and through other communication channels.

Putin has said that the main aim of the United States is ´to destroy strategic balance, to change the balance of power in such a way not just to dominate but to dictate their will to anyone´[89]. According to the Russian threat assessment, the enemy tries to destroy Russia's information sovereignty at the beginning of the war. If the enemy manages to destroy Russia's information sovereignty, it might be enough for the enemy to achieve victory[90]. To counter US supremacy in cyberspace, Russia has to improve its digital sovereignty. This means not only protection against viruses, attacks, illegal intrusion and theft of data, but also its capabilities to disconnect critical infrastructure from the global Internet[91].

The IS Doctrine states that foreign intelligence services are increasingly using cyberspace to destabilize the internal political and social situation of Russia. Foreign intelligence organizations are collecting intelligence information in and through cyberspace and targeting Russian government bodies, research organizations and enterprises of the military-industrial complex. Terrorist and extremist organizations are developing malware, which can be used against objects of Russia's critical information infrastructure. The amount of cybercrime is also increasing[92]. In addition, terrorists and extremist organizations are using cyberspace to foster interethnic and social tensions as well as spread extremist ideology.

[87] UP-646 (2016)

[88] Kamyshev, E, *Information Security and Protection of Information*. (Tomsk: Federalnoe Agenstvo RF po nauke i obrazovaniju 2009). (in Russian)

[89] Putin, Vladimir, Meeting of the Valdai International Discussion Club (22 October 2015). http://en.kremlin.ru/events/president/news/50548

[90] Yarovaya 2013

[91] Eliseev, Igor, 'I shooted with digital cannon', *Rossiyskaya Gazeta* No 6085 (109) (23 May 2013) (in Russian) https://rg.ru/2013/05/23/ashmanov.html

[92] UP-646 (2016)

The traditional Russian fear of being surprised and not completely defendable against an external enemy[93] has been extended to include internal enemies. The fear of internal disturbances, which has been prevalent in Russian leaders for centuries, has grown because of the so-called Arab Spring, which started in Tunisia in 2010. The Kremlin's fear of Western interference in Russian domestic affairs has increased during Putin's regime[94] and Russia feels that it faces real threats to its security in ´practically all spheres of its vital activities´[95]. Even in their public speech, Russian leadership considers the color revolutions in Arab countries and in Ukraine as being financed and coordinated by Western countries. They likely fear that there is a possibility of a similar revolution in Russia[96]. In 2004, Vladislav Surkov, the deputy director of the president's administration, stated that ´the enemy is at the gate, and not only at the gate because in the besieged town there is a fifth column of left and right radicals … sponsored by foreign states´ [97].

The Russian view is that the revolutions in Tunisia, Libya and Egypt were not spontaneous but were created and sponsored by Western intelligence services[98]. The Bolotnaya Square demonstrations in 2011 strengthened the belief of Kremlin that the West is attempting to destabilize Russia's internal situation by means of inspiring color revolutions. According to official Russian opinion, the West is trying to influence Russian internal affairs by creating and sponsoring an opposition movement and by supporting, for example, non-governmental organizations to oppose the regime. The Military Doctrine 2014 describes the subversive activities of special services and organizations of foreign states against Russia as an external military danger. Activities aimed at violent change, the constitutional system, and destabilizing the political and social situation in Russia are listed as internal military dangers in the Military Doctrine 2014.

Russian's own assessments of its technological inferiority[99] and of Western technological superiority[100] in cyberspace strengthen the country's perception of strategic vulnerability [101].

[93] Covington 2016

[94] Monaghan 2008

[95] Gusachenko, V., A., 'On the current context of the concept of national security', *Voennaya Mysl* 7 (2007) 2-13. (in Russian) http://militaryarticle.ru/voennaya-mysl/2007-vm/10032-ob-aktualnom-kontekste-ponjatija-nacionalnaja

[96] Facon 2016

[97] Ovtsarenko, Elena, 'Deputy Head of the Presidential Administration Vladislav Surkov: Putin is strengthening the state, not himself', Komsomolskaya Pravda (28 September 2004). (in Russian) https://www.kompravda.eu/daily/23370/32473/

[98] Skak 2016

[99] Covington 2016

[100] Facon 2017

[101] Covington 2016

According to the Information Society Strategy 2017, those states whose economy is based on the use of technologies for big data analysis have an advantage over other states. Furthermore, the technologies used in Russia are produced in the Western countries, not in Russia. The use of foreign ICT, especially in the objects of Russia's critical information infrastructure, pose a significant challenge for the country's cyber security management[102].

A lack of competitive Russian information technologies has domestic industry dependent on foreign information technologies, such as electronic components, software, computers, and telecommunications equipment. This dependence remains high, which makes the socio-economic development of the Russian Federation dependent on the geopolitical interests of foreign countries[103]. Some 90% of Internet-related functions and technology are invented, produced or implemented in the USA, and the USA is the only state that has comprehensive digital sovereignty[104].

The use of force and the efficacy of violence

The fundamental elements of a strategic culture reflect the central paradigm, that is, those assumptions about the nature and role of conflict and the enemy, the threat posed by the enemy, and about the use of force against these threats[105]. Russians, in Wirtz's formulation, are ´good Clausewitzians´, understanding that war is a political act and a continuation of politics. According to Wirtz, Russians manage to find the links between technology, military operations, strategy, and political outcomes, both despite and because of their lack of technological backwardness. [106] Russian leadership has had, and continues to have, a strong reliance on the military and on the use of force or other coercive means to achieve national interests[107].

A strong belief in the use of military force remains one of the fundamental factors in Russian strategic culture[108]. The military has been the main instrument in creating buffer zones and in controlling neighboring spaces and countries. In the Russian narrative, the military has been a barrier against invasion and a defender of the besieged fortress.

[102] UP-203 (2017)
[103] UP-646 (2016)
[104] Eliseev 2013
[105] Johnston 1995a:46
[106] Wirtz, James J, 'Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy', *CCDCOE Tallinn* (2015). https://ccdcoe.org/uploads/2018/10/Ch03_CyberWarinPerspective_Wirtz.pdf
[107] Facon 2016
[108] Igumnova 2011

The role of the security services has increased because of increased internal threats in the form of opposition sponsored by the West, terrorists, and extremists. Especially during Putin's third term, starting in 2012, the number of people in the security services, the so-called Chekists, has grown. This KGB culture within the Russian leadership and the Chekist threat perception centered on color revolutions has intensified the role of internal threats in Russian threat perception.[109]

Strategic Preferences in the Cyber Environment

According to Johnston, strategic preferences consist of ´assumptions at a more operational level about what options are the most efficacious for dealing with the threat environment as defined by the answers to the central paradigm[110]´. Russian strategic preferences in the cyber environment deal with threats similar to those in Russia's common threat environment. The same sense of vulnerability is seen in cyberspace as well. Western countries are using technical supremacy and challenging Russia with offensive cyberspace operations and by supporting internal opposition. Russian strategic preferences to deal with these threats in cyberspace are improved protection of critical information infrastructure, a pivot to digital sovereignty by isolating RUNET from the global Internet, increasing surveillance of RUNET, and improving legal interception capabilities to control opposition, banning user anonymity online, the substitution of ICT imports with Russia's own hardware and software production, and international cyber security agreements.

To improve protection of the country's critical information infrastructure, Russia is building a combined information security system called GosSOPKA[111]. The GosSOPKA system is a combined, territorially distributed complex that includes forces and means for detecting, preventing and eliminating the consequences of computer attacks and responding to computer incidents. The information resources of the Russian Federation are understood as information systems, information and telecommunications networks, and automated management systems located in the territory of the Russian Federation as well as in the diplomatic missions and

[109] Facon 2016; Skak 2016; Kolesnikov 2016
[110] Johnston,1995b: ix–x, 248
[111] UP-203 (2017)

consular offices of the Russian Federation[112]. The FSB is tasked with operating the GosSOPKA system[113].

To counter the external cyber threat and keep the Russian segment of Internet stable and independent, Russia is developing a national system of the Internet[114] called RUNET. According to Ashmanov, to counter the USA's supremacy in cyberspace, Russia must improve its digital sovereignty, stability, and security.[115] Russia's functioning integrated telecommunications network should be stable and safe in peacetime, in the event of a direct threat of aggression, and in wartime[116]. This means not only protection against viruses, attacks, illegal intrusion, and theft of data, but also capabilities to disconnect critical infrastructure from the global Internet[117]. The Ministry of Communications Information Society program aims to have 99% of RUNET traffic transferred inside Russian borders by 2020. Part of this plan is to duplicate 99% of RUNET's critical infrastructure within Russia[118].

Increasing surveillance of RUNET and improving legal interception capabilities is part of the battle against internal threats in RUNET. This has increased the role and mandate of security services in cyberspace. The FSB has a mandate to monitor RUNET traffic. The tool for FSB Internet surveillance is the System for Operative Investigative Activities (SORM). Since the 1990s, the operational capabilities of SORM systems have been improved from SORM 1 to SORM 3. SORM 1 collected mobile and fixed line telephone calls. SORM 2 began collecting Internet traffic. SORM 3 collects all kinds of communication on social networks, Wi-Fi, e-mails, Internet traffic, mobile calls, and voice-over-Internet. SORM 3 was introduced into operative use in 2014[119]. Internet service providers (ISP) are required to provide the FSB with statistics on all Internet traffic that passes through their servers. ISPs are also required to install

[112] UP-31 (2013) Decree 31 of the President of the RF of 15 January 2013 on the establishment of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation. (in Russian) https://rg.ru/2013/01/18/komp-ataki-site-dok.html

[113] UP-620 (2017) Decree of the President of the Russian Federation of December 22, 2017 No. 620 on the improvement of the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation. (in Russian) http://www.kremlin.ru/acts/bank/42623

[114] UP-646 (2016)

115 Yarovaya 2013

116 UP-646 (2016)

117 Eliseev 2013

118 Meduza, 'Russia's Communications Ministry plans to isolate the RuNet by 2020'. (13 May 2016). https://meduza.io/en/news/2016/05/13/communications-ministry-plans-to-isolate-runet-by-2020

119 Soldatov Andrei, Borogan Irina, The Red Web (New York: Public Affairs 2015)

SORM devices on their servers, routing all transmission in real time through the FSB's local offices[120].

Traditionally, the military has been the one of maintain the idea of permanent war. This new war, however, is increasingly being fought within Russia against terrorists and groups labeled extremists and within information sphere, that is, in environments where traditional military force is not easily applicable, the role of non-military part of Russia's security organization has grown. The role of the FSB has grown in importance because it is the main actor in the war on terrorism and the defense of Russian networks. Another important actor in this permanent low-intensity war is military intelligence, the GU (previously known as the GRU).

In summer, 2017 Putin signed two laws to ban user anonymity on RUNET. Owners of virtual private network (VPN) services and Internet anonymizers are prohibited from providing access to websites banned in Russia. Roskomnadzor has authorization to block sites that provide instructions on how to circumvent government blocking[121]. Companies registered in Russia as ´organizers of information dissemination,´ including online messaging applications, are prohibited from allowing unidentified users. Those companies are required to identify their users by their cell phone numbers, and the government is tasked with elaborating the identification procedure. Mobile applications that fail to comply with requirements to restrict anonymous accounts will be blocked in Russia[122].

Digital sovereignty requires that Russia to have its own ICT production chain, hardware and software, search engines and browsers, network components, Russian-made Internet surveillance tools, monitoring and information security systems, a national segment of Internet social networks, and national payment systems[123]. Putin stated that Russia needs to build its own digital platforms, ones that should be compatible with the global information space[124].

According to the IS Doctrine 2016, the information security of Russia is characterized by a lack of competitive information technologies and the inadequate use of information technologies in the production of goods and services. The level of dependence of Russian industry on

[120] PP-538 (2005) Decree 538 of the Government of the Russian Federation of 27 August 2005 on Approval of the Rules for Interaction of Communication Operators with Authorized State Bodies Conducting Operational-Investigation Activities. (in Russian) http://www.consultant.ru/document/cons_doc_LAW_55326/

[121] FZ-276 (2017) Federal Law 276 of 29 July 2017 on Amendments to the Federal Law On Information, Information Technologies and Information Protection. (in Russian) https://rg.ru/2017/07/30/fz276-site-dok.html

[122] FZ-241 (2017) Federal Law 241 of 29 July 2017 on Amendments to Articles 101 and 154 of the Federal Law on Information, Information Technologies and Information Protection. (in Russian) https://rg.ru/2017/08/04/informacia-dok.html

[123] Yefremov, Alexey, Formation of the concept of state information sovereignty. (March 2017). (in Russian) doi: 10.17323/2072-8166.2017.1.201.215

[124] Putin, Vladimir, President's Speech to the Federal Assembly (1 March 2018). (in Russian) http://kremlin.ru/events/president/news/56957

western IT software and hardware is high. One of the strategic preferences to answer this technical backwardness in information technology is, according to the IS Doctrine 2016[125], to develop the country's IT sector by improving its own research, development and production of information technology. The previous information security doctrine from 2000 names the underdevelopment and backwardness of Russian information technology as a threat to the country's information security. Over the past decade, however, Russia has not managed to reduce the lead of Western countries in this area. The insufficient level of development of domestic information technology, services, and production capabilities continue to generate dependence on foreign information technology. According to the Russian assessment in 2013, Russia was three to five years behind the USA in ICT technology and only the USA had digital sovereignty[126].

One strategic preference of Russian strategic culture in the cyber environment is Russia's pivot to establish an international information security system for regulation of how information technologies are used for military and political purposes or for terrorist, extremist, criminal or other illegal purposes[127].

Conclusion

The status of cyber weapons in the field of international law today is equivalent to the status of nuclear weapons before the Limited Test Ban Treaty and Strategic Arms Limitations Treaties in the 1960s and 1970s. In other words, these weapons systems lack sufficient rules of engagement that, when combined with the fast pace of technological development, makes the cyber threat a serious security policy issue. With the acknowledgement of this special status of cyber weapons, it can be argued that the Cold War era theories of threat perception and the use of force can be applied to study and analyze these phenomena in cyberspace.

The interest in cyber warfare has created a need for theoretical tools to research cyber threats and responses to these threats. As we have argued in this paper, the theory of strategic culture is a suitable tool to explore and explain the formation of Russian cyber threat perception. The theory of strategic culture tries to identify the factors that are characteristic for national decision-making and state practice and to study how and why these factors influence such decisions and practices. Factors with an influence on Russian strategic thinking include historical,

[125] UP-646 (2016)
[126] Eliseev 2013
[127] UP-646 (2016)

geopolitical, religious or ideological ones. Elements of Russian strategic culture, such as a sense of vulnerability, the narrative of Russia as a besieged fortress, the mythology of permanent war, and technological inferiority can also be identified in Russian cyber threat perception.

The theory of strategic culture can also be used to explore and to explain Russian defensive cyber operations, based on its cyber threat perception, as well as the country's offensive cyber operations, such as cyber attacks and cyber espionage.

REFERENCES

Adamsky, Dima, 'Cultural Underpinnings of Current Russian Nuclear and Security Strategy', in J.L. Johnson, Kerry Kartchner and Marilyn Maines (eds) *Crossing Nuclear Thresholds. Leveraging Sociocultural Insights into Nuclear Decisionmaking. (*NY: Palgrave Macmillan 2018)

Aron, Leon, 'The Problematic Pages. In memory of Alexander Solzhenitsyn', *The New Republic*. (24 September 2008). https://newrepublic.com/article/62070/the-problematic-pages

Berrett, Matthew T and Johnson, Jeannie L, 'Cultural Topography: A New Research Tool for Intelligence Analysis — Central Intelligence Agency.', *Studies in Intelligence* Vol. 55, No. 2 (June 2011) https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-2/pdfs-vol.-55-no.-2/Berrett-Cultural%20Topography-9June2011.pdf

Bloomfeld, Alan, 'Time to Move On: Reconceptualizing the Strategic Culture Debate.' *Contemporary Security Policy* 33(3) (Dec 2012) 437-461. doi: 10.1080/13523260.2012.727679

Bolden, Micah-Sage and Nalla, Mahesh, 'Theorizing Cybercrime: Applying Routine Activities Theory.' (2014). https://www.academia.edu/8897451/Theorizing_Cybercrime_Applying_Routine_Activities_Theory

Booth, Ken, 'Strategic Culture: Validity and Validation', *Oxford Journal on Good Governance* 2, no. 1 (2005), 25-28.

Cirenza, Patrick, 'The Flawed Analogy Between Nuclear and Cyber Deterrence', *Bulletin of the Atomic Scientists* (2016 February 22). http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179

Covington, Stephen R. 'The Culture of Strategic Thought Behind Russia's Modern Approaches to Warfare.' *Belfer Center. Harvard Kennedy School.* (2016). https://www.belfercenter.org/sites/default/files/files/publication/Culture%20of%20Strategic%20Thought%203.pdf

Davis Cross, Mai´a K, 'Rethinking epistemic communities twenty years later', *Review of International Studies* Vol 39, Issue 1 (Jan 2013), 137-160. doi: 10.1017/S0260210512000034

Desch, Michael C, 'Culture Clash: Assessing the Importance of Ideas in Security Studies', *International Security* Vol. 23, No. 1 (Summer, 1998), 141-170.

Echevarria II, Antulio J and Hoffman, Frank, 'Review Essay - Strategic Culture And Ways Of War, Elusive Fiction Or Essential Concept?', *Naval War College Review*: Vol. 70 : No. 2 , Article 7 (2017). https://digital-commons.usnwc.edu/nwc-review/vol70/iss2/7

Eliseev, Igor, 'I shooted with digital cannon', *Rossiyskaya Gazeta* No 6085 (109) (23 May 2013) (in Russian) https://rg.ru/2013/05/23/ashmanov.html

Facon, Isabella, 'Russian Strategic Culture in the 21st Century: Redefining the West-East Balance', in Tellis A, Szalwinski A and Wills M (eds) *Understanding Strategic Cultures in the Asia-Pacific*, *Strategic Asia 2016-2017*, The National Bureau of Asian Research, (2016) 62-89. http://nbr.org/publications/strategic_asia/pdf/SA16_ExecutiveBrief.pdf

Facon, Isabella, 'Russia's national security strategy and military doctrine and their implications for the EU', *European Parliament's Sub-Committee on Security and Defence* (2017). http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/578016/EXPO_IDA(2017)578016_EN.pdf

Felgenhauer, Pavel, 'Russia's Imperial General Staff', *Perspective.* Volume XVI Number 1 (October- November 2005). https://www.bu.edu/iscip/vol16/felgenhauer.html

FZ-172 (2014) Federal Law 172 of 28 June 2014 on Strategic Planning in the Russian Federation. https://rg.ru/2014/07/03/strategia-dok.html

FZ-241 (2017) Federal Law 241 of 29 July 2017 on Amendments to Articles 101 and 154 of the Federal Law on Information, Information Technologies and Information Protection. (in Russian) https://rg.ru/2017/08/04/informacia-dok.html

FZ-276 (2017) Federal Law 276 of 29 July 2017 on Amendments to the Federal Law On Information, Information Technologies and Information Protection. (in Russian) https://rg.ru/2017/07/30/fz276-site-dok.html

Gerasimov, Valeri, 'The value of science in anticipation. New challenges require rethinking the forms and methods of conducting military operations', *Voenno-Promyshlennyi Kurier* (26 February 2013). (in Russian) https://www.vpk-news.ru/articles/14632

Gray, Colin S., 'What Rand Hath Wrought', *Foreign Policy*. No 4, (Autumn 1971), 118.

Gray, Colin S., 'Strategic Culture as Context: The First Generation of Theory Strikes Back.' *Review of International Studies.* Vol 25, No. 1 (Jan 1999), 49-69.

Gray, Colin, S., 'Out of the Wilderness: Prime-time for Strategic Culture'*, Inaugural speech made at the Defense Threat Reduction Agency* (October 2006). https://fas.org/irp/agency/dod/dtra/stratcult-out.pdf

Gusachenko, V., A., 'On the current context of the concept of national security', *Voennaya Mysl* 7 (2007) 2-13. (in Russian) http://militaryarticle.ru/voennaya-mysl/2007-vm/10032-ob-aktualnom-kontekste-ponjatija-nacionalnaja

Horton-Eddison, Martin, 'Is Theory of Strategic Culture Valid?' (2018). https://www.academia.edu/12536463/Is_the_Theory_of_Strategic_Culture_Valid

Howlett D & Glenn J . 2005. Nordic strategic culture. Cooperation and conflict, 40 (1), 121–140. https://journals.sagepub.com/doi/10.1177/0010836705049737

Igumnova Lyudmila, 'Russia's Strategic Culture Between American and European Worldviews', *The Journal of Slavic Military Studies,* Volume 24 (2011). doi: 10.1080/13518046.2011.572729

Jaishankar, K, 'Establishing a Theory of Cyber Crimes', *International Journal of Cyber Criminology* Vol 1 Issue 2 (July 2007). http://www.cybercrimejournal.com/Editoriaijccjuly.pdf

Johnson, Jeannie L, 'Conclusion: toward a standard methodological approach', in Johnson, Jeannie L., Kerry M. Kartchner, and Jeffrey A. Larsen, *Strategic culture and weapons of mass destruction. Culturally based insights into comparative national security policymaking*. (NY: Palgrave Macmillan 2009).

Johnston, Alistair, 'Thinking about Strategic Culture', *International Security* Vol. 19, No. 4 (Spring, 1995a), 32-64. http://www.fb03.uni-frankfurt.de/45431264/Johnston-1995-Thinking-about-Strategic-Culture.pdf

Johnston, Alistair, Cultural Realism: Strategic Culture and Grand Strategy in Chinese History. (New Jersey: Princeton University Press 1995b)

Kamyshev, E, *Information Security and Protection of Information*. (Tomsk: Federalnoe Agenstvo RF po nauke i obrazovaniju 2009). (in Russian)

Kennan, George, 'The Sources of Soviet Conduct', *Foreign Affairs* 25 (1947), 566-82. https://is.muni.cz/el/1423/jaro2017/BSS185/um/Week_4_Kennan_on_Containment.pdf

Kerry, John, F, *Hearing before the Committee on Foreign Relations of United States*. (January 24, 2013) https://www.gpo.gov/fdsys/pkg/CHRG-113shrg86451/pdf/CHRG-113shrg86451.pdf

Kolesnikov, Andrei, 'Do Russians Want War?', *Carnegie Moscow Center* (June 2016). http://carnegieendowment.org/files/Article_Kolesnikov_2016_Eng-2.pdf

Komarov, Aleksei, 'Normative documents on the safety of automated control systems and critical information infrastructure' (21 July 2016). (in Russian) http://www.securitylab.ru/blog/personal/zlonov/144489.php

Lantis, Jeffrey, S, 'Strategic Culture and National Security Policy', *International Studies Review* Vol. 4, No. 3 (Autumn, 2002), 87-113. Available at: http://www.fb03.uni-frankfurt.de/45431305/Lantis-2002--Strategic-Culture-and-National-Security-Policy.pdf

Lantis, Jeffrey, S, 'Presentation on theme: Strategic Culture and Threat Assessment', *Second Annual Joint Threat Anticipation Center Workshop,* The University of Chicago (4 April 2006.) Available at: http://slideplayer.com/slide/4271931/

Lapina M, Revin A & Lapin V, Информационное право [Information Law] (Moscow: Zakon i pravo 2004)

Libel, Tamir, 'Explaining the security paradigm shift: strategic culture, epistemic communities, and Israel's changing national security policy', *Defence Studies* (March 2016), 137-156. DOI: 10.1080/14702436.2016.1165595

Lock, E. 2018. Strategic Culture Theory: What, Why, and How. http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-320#acrefore-9780190228637-e-320-div1-2

Meduza, 'Russia's Communications Ministry plans to isolate the RuNet by 2020'. (13 May 2016). https://meduza.io/en/news/2016/05/13/communications-ministry-plans-to-isolate-runet-by-2020

MFA, *Foreign Policy Concept of the Russian Federation* (30 November 2016.) http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248

MoD, *Military Doctrine of the Russian Federation* (2014). https://rg.ru/2014/12/30/doktrina-dok.html

Monaghan, Andrew, ''An enemy at the gates' or 'from victory to victory'?', *Russian foreign policy. International Affairs* 84(4) (2008), 717-733. http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2346.2008.00734.x/abstract

Murray, Williamsson, 'Does Military Culture Matter?', *Orbis* Volume 43, Issue 1 (Winter 1999), 27-42. https://doi.org/10.1016/S0030-4387(99)80055-6

Nato, Warsaw Summit Communiqué of the North Atlantic Council in Warsaw (8-9 July 2016). https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Orlov, Vladimir, Start of new battles, *Moskovskie Novosti*. (21 April 2011). (in Russian). http://www.mn.ru/newspaper/world/68636

Ovtsarenko, Elena, 'Deputy Head of the Presidential Administration Vladislav Surkov: Putin is strengthening the state, not himself', Komsomolskaya Pravda (28 September 2004). (in Russian) https://www.kompravda.eu/daily/23370/32473/

Poore, Stuart, 'What is the context? A reply to the Gray-Johnston debate on strategic culture', *Review of International Studies* 29 (2003), 279-284. DOI: 10.1017/S0260210503000172

PP-538 (2005) Decree 538 of the Government of the Russian Federation of 27 August 2005 on Approval of the Rules for Interaction of Communication Operators with Authorized State Bodies Conducting Operational-Investigation Activities. (in Russian) http://www.consultant.ru/document/cons_doc_LAW_55326/

Putin, Vladimir, Meeting of the Valdai International Discussion Club (22 October 2015). (in Russian) http://en.kremlin.ru/events/president/news/50548

Putin, Vladimir, President's Speech to the Federal Assembly (1 December 2016). (in Russian) http://kremlin.ru/events/president/news/53379

Putin, Vladimir, President's Speech to the Federal Assembly (1 March 2018). (in Russian) http://kremlin.ru/events/president/news/56957

Pynnöniemi, Katri, 'Russia's National Security Strategy: Analysis of Conceptual Evolution', *The Journal of Slavic Military Studies* 31:2 (2018) 240-256.

Rogozin, Dmitri, Speech by Dmitry Rogozin at a press conference in the "RG" (28 June 2013). (in Russian) https://rg.ru/2013/06/28/doklad.html

Sinovets, Polina, 'From Stalin to Putin: Russian Strategic Culture in the XXI Century, Its Continuity, and Change', *Philosophy Study* Vol. 6, No. 7 (July 2016), 417-423 doi: 10.17265/2159-5313/2016.07.002

Skak, Mette, 'Russian strategic culture: the role of today's chekisty', *Contemporary Politics*. Vol. 22, Iss. 3 (2016), 324-341. doi: 10.1080/13569775.2016.1201317

Snyder, Jack, *The Soviet Strategic Culture : Implications for Limited Nuclear Operations* (Santa Monica, CA: RAND Corporation, 1977). https://www.rand.org/pubs/reports/R2154.html.

Soldatov Andrei, Borogan Irina, *The Red Web* (New York: Public Affairs 2015)

UP-31 (2013) Decree 31 of the President of the RF of 15 January 2013 on the establishment of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation. (in Russian) https://rg.ru/2013/01/18/komp-ataki-site-dok.html

UP-203 (2017) Decree 203 of the President of the RF of 9 May 2017. On the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030]. (in Russian) http://kremlin.ru/acts/bank/41919

UP-569 (2017) Decree 569 of the President of the RF of 25 November 2017 on Amendments to the Regulations on the Federal Service for Technical and Export Control. (in Russian) http://kremlin.ru/acts/bank/42489

UP-620 (2017) Decree of the President of the Russian Federation of December 22, 2017 No. 620 on the improvement of the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation. (in Russian) http://www.kremlin.ru/acts/bank/42623

UP-646 (2016) Doctrine of Information Security of the Russian Federation. (in Russian) https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

UP- 683 (2015) Presidential Decree 683 of December 2015 on the National Security Strategy of the Russian Federation. (in Russian) http://pravo.gov.ru/proxy/ips/?docbody=&nd=102385609

Wirtz, James J, 'Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy', *CCDCOE Tallinn* (2015). https://ccdcoe.org/uploads/2018/10/Ch03_CyberWarinPerspective_Wirtz.pdf

Zhuang, Rui; Bardas, Alexandru; DeLoach, Scott & Ou, Xinming, 'A Theory of Cyber Attacks A Step Towards Analyzing MTD Systems', *MTD'15 Denver CO USA* (12 October 2015). doi: 10.1145/2808475.2808478.

Yarovaya, M, 'Igor Ashmanov: 'Today information domination is the same as air superiority'', (1 May 2013). (in Russian) https://ain.ua/2013/05/01/igor-ashmanov-segodnya-informacionnoe-dominirovanie-eto-vse-ravno-chto-gospodstvo-v-vozduxe

Yefremov, Alexey, Formation of the concept of state information sovereignty. (March 2017). (in Russian) doi: 10.17323/2072-8166.2017.1.201.215