Theory of strategic culture : An analytical framework for Russian cyber threat perception

Kari, Martti J.

Routledge
2023

Kari, M J & Pynnöniemi, K 2023, 'Theory of strategic culture : An analytical framework for Russian cyber threat perception', Journal of Strategic Studies, vol. 46, no. 1. https://doi.org/10.1080/01402390.2019.

http://hdl.handle.net/10138/571479
10.1080/01402390.2019.1663411

acceptedVersion

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 defence 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

Kari, M. J., & Pynnöniemi, K. (2019). Theory of strategic culture: An analytical framework for Russian cyber threat perception. Journal of Strategic Studies. https://doi.org/10.1080/01402390.2019.1663411

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 paralyse 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 defence 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 behaviour 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 behaviour. In the early 1980s, many researchers argued that the USA was incapable of

---

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

thinking and acting strategically, and the Soviet Union, as a Clausewitzian and militarily oriented 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,

---

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

and by following and understanding the argumentation between different groups (i.e., between 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

---

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).

been refuted. As one of the theorists of the first generation, Colin Gray, has said, "strategic 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 behaviour, 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 behaviour. Another advantage is that strategic culture considers state-specific factors, which influence state behaviour. 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

---

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

can also 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 behaviour in practice. Russian state behaviour 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 behaviour 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

---

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/

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

´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´ 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

38 Johnston, 1995a: 46
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

operational doctrine. Auto communication symbols, myths and strategies do not have an effect on the strategic behaviour 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 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 defence 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 behaviour 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 behaviour. 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 behaviour rather than explain the cause of that behaviour. 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 behaviour.

This article follows Johnston's idea about the disjunction of strategic culture from state behaviour. State behaviour 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.

---

[43] Johnston, 1995a: 57
[44] Johnston, 1995a: 55
[45] Gray 1999

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 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, 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:

---

[46] Johnston 1995b
[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

- 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

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 defence 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

---

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

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 defence of the country and all 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 behaviour 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.

---

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

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 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 deci-

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

sions 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)
- 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

[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)

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]. 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]

---

[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)

[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

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 private 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].

---

[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

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 establishing 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]

---

[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

[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)

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].

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 defence 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.

---

[85] UP-646 (2016)
[86] Johnston 1995a: 46

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, provoking 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

---

[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

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.

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

---

[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)
[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

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]. 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,

---

[99] Covington 2016
[100] Facon 2017
[101] Covington 2016
[102] UP-203 (2017)
[103] UP-646 (2016)
[104] Eliseev 2013

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.

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

---

[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
[109] Facon 2016; Skak 2016; Kolesnikov 2016
[110] Johnston,1995b: ix–x, 248

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 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 programme 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

---

[111] UP-203 (2017)
[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

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 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 defence 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].

---

119 Soldatov Andrei, Borogan Irina, The Red Web (New York: Public Affairs 2015)

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

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 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

---

[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

125 UP-646 (2016)

126 Eliseev 2013

127 UP-646 (2016)

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 analyse 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, 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), 255.

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*. (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), 244.

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