# Cyber deterrence and Russia's active cyber defense

PhD student, Maija Turunen
Finnish National Defence University
Helsinki
Finland
maija.turunen@ftia.fi

PhD, Colonel (ret) Martti J Kari
Jyväskylä University
Finland
martti.j.kari@jyu.fi

Abstract:

The Russian Military Doctrine (2014), the National Security Strategy (2015), and the Information Security Doctrine (2016) consider the information space as a domain of warfare, where the war against Russian digital sovereignty is waged. Russia's cyber defense includes the 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. Yet a credible defense also requires credible deterrence. The traditional deterrence options are deterrence by punishment, deterrence by denial and deterrence by entanglement. Deterrence by punishment is based on a defender's capability to retaliate. Deterrence by denial means that a defender is capable to limit damages by denial attacker´s success. Deterrence by entanglement is based on nations' mutual interest and their political, economic, and strategic interdependence. An effective deterrence strategy has to be credible, based on capability and send the right message to a possible adversary. Credibility means that the state displays the willingness to counteract an attack, and capability means that the state has the tools to do so.

Cyber warfare differs from warfare in other domains because actors in cyber conflicts are not always military actors. State actors, criminals, and terrorists attack state authorities, media, and critical infrastructure. The attribution of an attack to a specific party is often difficult or impossible to do. An attacker in cyberspace can act with deniability, impunity, and anonymity. Traditional deterrence is difficult or impossible to implement in cyberspace because denial can be too difficult and there is no possiblity to identify an attacker for retaliation. The strategic option of cyber deterrence is an active cyber defense, which is a combination of deterrence by denial and deterrence bypunishment.

This paper discuss Russian active cyber defense, which combines defensive and offensive cyber capabilties. In its theoretical context, this paper is based on the theory of deterrence and the theory of strategic culture. The theory of deterrence is used to describe how Russia constructs its cyber deterrence. The theory of strategic culture seeks to explain Russia's motives for these choices.

Keywords: Russia, cyber deterrence, strategic culture, active cyber defense

## 1. Introduction

Most industrial countries are preparing for cyber warfare, while some countries are already waging these wars. In the Western debate, cyber warfare is used more as an independent concept (McCulloh & Johnson 2013 pp. 5-14), while in Russia it is seen as part of information warfare (Hathaway & Klimburg 2012, 17-18; Nye 2017, 49). States are seeking to increase both their defensive and offensive cyber capabilities as well as to create deterrence of adversaries. To this end, states are using strategic communication to deter potential attackers, and different official documents, such as strategies and doctrines, are an important part of this communication. These documents disclose how the state publicly understands its position in cyberspace and communicates its goals and capabilities there. Creating a cyber deterrent is thus part of the effort to influence an adversary's war character.

The concept of deterrence is traditionally derived from the concept of nuclear deterrence, but it is not functional in the cyber world. According Manjikian (2016, 16) there are the knowledge problems or the problem of attribution; the temporal problem, or the ways in which time functions in cyberspace as opposed to during nuclear attacks; the payoff or reward structure for both types of events.

Cyber deterrence can be seen to consist of the capabilities of the actor (state/adversary), the willingness to use them, and the image that this state manages to project to its potential adversaries. Adversaries' cultural, political, and ideological background and their perception of the prevailing character of war affect how credible this cyber deterrent is. According to Goodman (2010, 105), deterrence has eight elements: an interest, a deterrent declaration, denial measures, penalty measures, credibility, reassurance, fear, and a cost–benefit calculation.

The use of cyber methods is suitable for the implementation of the basic principles of Russian strategic psychological thinking, like surprise and confusion. Similarly, with the use of these methods of subtle nature and the fact that the methods are left to speculation, these methods are well suited as a means of influencing the so-called grey area, in the initial period of war, where some Russian war theorists (Chekinov & Bogdanov, 2012) claim that wars in the future will be won . These grey areas can be considered as the new normal in both Russian and Western military strategic and deterrence thinking.

## 2. Theories in the background

In its theoretical context, this paper is based on the theory of deterrence. In international politics, deterrence theory is the idea that a state, owning destructive power, could deter a more powerful adversary with this destructive power. Generally, deterrence means preventing an adversary from taking undesired action. The general theory of deterrence is defined as the use of means of decisive influence over an adversary's decision-making. Traditional deterrence is based on an adversaries' perception that a threat of retaliation exists, or the planned attack or other action cannot be successful or the costs of the attack outweigh the benefits. (Jasper, 2018, 161) Further, Goodman (2010, 108) highlights that "in addition to strong denial measures, classical deterrence theory demands that penalty measures be certain, severe, and immediate; however, cyber deterrence emphasizes certainty more so than severity or immediacy." Three traditional deterrence options are deterrence by punishment, deterrence by denial and deterrence by entanglement. In addition, one can also talk about deterrence by association, deterrence by norms and taboos.

Deterrence by punishment or by retaliation is based on a defender's capability to first identify the attacker and then to retaliate against the adversary's hostile activity. Deterrence by punishment means, in the kinetic world, the capability to create a credible threat to an adversary, even with a deadly response

that can cause unexpected losses. In cyberspace, it is more challenging to define an adversary's hostile activity, which gives the right to retaliate than it is in other domains. Identifying the cyber threat is challenging due to the attribution of the attacker, the infinite number of constantly changing actors, the irrelevance of geographical distance between the target and the attacker, and the likelihood of an attacker's plausible deniability (Mandel, 2017, 5). According to Kello (2014, 144), the problem with deterrence by punishment is also: "The difficulty of attaining credible attribution of the identity and location of an assailant degrades the crucial psychological base of the logic of penalties. The difficulty inheres in the opaqueness of cyberspace, but it is also concerns the traditional sate-centric procedures of international relations."

Deterrence by denial is a defensive strategy that tries to convince an adversary that an attack is futile, because it would not achieve successful and cost-effective results. Deterrence by denial means that a defender is capable of limiting damages and withholding benefits of malicious activity by denial of attacker's success. The denial of an attacker's success is implemented by ensuring the security of the target of the attack. In cyberspace, this denial is realized by increasing the security of information systems, information and telecommunication networks, and automatic control systems (Jasper, 2017, 15). One of the ways to increase the security of information systems is to use so-called defense-in-depth, consisting of multiple layered, overlapping and mutually supportive defense systems, which includes detective and preventive functionalities. In practice, this means increased capability to detect a cyber-attack and respond to an attack as well as to reduce and mitigate risk (Pescatore & Sager, 2013). A well-planned and implemented cyber defense can detect and repulse the majority of cyber-attacks. According to Kello (2014, 143-144) the deterrence by denial involves the following types of problems as if the impossibility of reducing the full effects of cyberattack impedes denial by means of redundancy and resilience and these indirect effects are largely unknowable before attack.

Deterrence by entanglement is based on nations' mutual interest and political, economic, commercial, and strategic interdependence in cyberspace as well as some degree of vulnerability (Jasper, 2018, 198, 234, 269). Mutual interest means a common reliance on the Internet that unites otherwise non-friendly, competing or even hostile states and actors. These actors refrain from attacking each other because they gain, for example, financially due to the Internet connectivity (Ryan, 2017). Mutual interest is at the core of the concept of deterrence by entanglement and it expands to include other methods of deterrence, such as encouraging responsible state behavior through norms and taboos. Nye (2017, 59) has stated, that: "Entanglement is sometimes called "self-deterrence" and treated as a case of misperception. The term "self-deterrence," however, should not lead one to dismiss the importance of entanglement, whether in a bilateral or a general sense. The perceptions that costs will exceed benefits may be accurate, and self-restraint may result from rational calculations of interest."

According to Kari (2019, 25), 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. Johnston defines strategic culture as a set of historical patterns of how state leadership thinks about the use of force to achieve political goals. According to him, 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). 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 paper applies Johnston's definition of strategic culture and his methodological framework. The central paradigm of Russian strategic culture corresponds to the Russian threat perception and strategic preferences correspond to Russia's deterrence by denial in cyberspace.

3. An active and effective cyber defence and deterrence

Denning and Strawser (2017, 194-195) defines an active and passive cyber defence as follows: "Active cyber defense is a direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats against friendly forces and assets, and passive cyber defense is all measures, other than active cyber defense, taken to minimize the effectiveness of cyber threats against friendly forces and assets. Put another way, active defenses are direct actions taken against specific threats, while passive defenses focus more on protecting cyber assets from a variety of possible threats." Denning (2013, 3) has argued, that: "Active cyber defenses can be characterized by four features: scope of effects, degree of cooperation, types of effects, and degree of automation. Together, they place active cyber defenses in a four-dimensional space and provide a framework for distinguishing different types of active cyber defenses and analyzing the ethical issues they raise."

The strategy of active cyber defence is based upon the real-time detection and analysis of network security breaches seeks to create a comprehensive, automated and thereby unavoidable response to neutralize and reinforce the effects automatically through associated auto trigger of legal simultaneous countermeasures inside and beyond network and state territorial boundaries. The remedies for this are cyber threat intelligence, real-time detection of intrusion and analysis of network security breaches. The offensive part of active cyber defense includes the capability to give early warning of a possible cyber-attack, that is, to reveal and identify the cyber threat and respond to the incoming cyber-attack in the early stages of the cyber kill chain to withstand the attack. The exact attribution of the attacker is not always vital for the response. Rather, it is more important to stop the attack before damage occurs (Jasper, 2017, 207- 209; Mandel, 2017, 35).

Effective deterrence requires capability, credibility, and communication. Deterrence operates in a grey area. Escalation into war means that deterrence has failed. Strategic communication can compensate for the shortcomings of capability, but not the loss of credibility. Because deterrence rests on perceptions, its effectiveness depends on credibility. An effective deterrence strategy should be credible from the perspective of the actor that is to be deterred. Effective deterrence should be based on capability and it should transmit the correct and intended message to the desired audience. Credibility means that the state shows the willingness to employ proposed actions to counteract the attack while capability means that the state has the capability and tools to do so (JP 3-0, 2017). That means offensive capabilities, which may be possessed by the state itself or its allies. Passive defense alone will not work.

4. Russian version of an active cyber deterrence

According to the Russian view, 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 internally as well. Terrorists and extremists may direct

cyberspace attacks at 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 RBA, 2013; SBRF, 2013; MDRF, 2014). The Russian view about deterrence and its functions in warfare is not a mainstream view in West. For example the development of a multistakeholder approach in which the state's interests are not dominant, does not happen. From the Russian point of view, it is always a question of Russian government`s interest and national security. These values take precedence over everything else, and it is up to the stakeholders to implement them in a manner defined by the authorities.

Russia has tried to improve cyber deterrence by punishment, deterrence by denial, and by the combination of deterrence by association, deterrence by norms and taboos, and deterrence by entanglement. Russia is building an active cyber deterrent as part of its other deterrent systems by all available means. Indeed, Bērziņš (2019, 166–167) considers that the Russians have placed influence at the center of their operational planning. Examples of such influence include skillful internal communication, masking operations, psychological operations, and well-constructed external communication. Strategically, therefore, the operational nature of the new war cannot be regarded as a military campaign in the classic sense of the term, but as an opportunistic combination of different strategies. Bērziņš also emphasizes that the key to understanding Russia's strategy is to understand that it is eclectic and relies on whatever works in a given situation.

One important part of communication about effective deterrence are Russian military strategies and doctrines. In particular, they emphasize the various threats and recognize and oblige them to respond strongly to these threats in all domains. They also contain clear cyberspace management measures. The Russian Military Doctrine not only has the function to guide the planning, operation and legislation of the authorities, but it also serves as a tool for strategic communication. The Military Doctrine creates strategic deterrents against those who threaten the state, while also communicating to Russian citizens about threats to the state and justifying the means of defending against such threats. As in his speech in 2017, General Gerasimov (Komsomolskaya Pravda, 2017), the General Staff Commander of the Russian Army, seems to focus on the fight in the minds of the citizens, the sixth dimension of battlefields. Gerasimov stated that victory is not only achieved through material resources, but also through the nation's intellectual resources, its cohesion, and the unification of all forces to resist aggression.

The doctrine lists the neutralization of potential military threats by political, diplomatic, and other non-military means. However, the doctrine, in paragraph 21s), includes an important additional measure, even with offensive features: "creating conditions that reduce the risk of using information and communication technology to achieve military policy goals." This may be seen as referring primarily to political diplomatic means to influence, for example, international law, but also to empowering the armed forces to take action to eliminate targets that increase such risks.

In the Russian philosophy of warfare, concealment and deception play an important role. These elements are also central to cyber operations, along with the control of intangible agents and service providers by Russian security service authorities. The coordinated role of such service providers in close proximity to state actors is an essential and likely growing component of both Russian cyber capability and other operational warfare, while maintaining the traditional leading role and mission of traditional armed forces. Using service providers is not always an active operational choice, but allowing them to serve their own strategic and tactical goals in Russia may obscure the adversary's situation awareness and create uncertainty, which may open up new opportunities for state actors or contribute to action by state actors to deceive and conceal their own operations. One of Russia's most important tasks is to assess and forecast

the development of the global and regional conflicts and military policy using modern technical tools and information technology in order to curb and prevent military conflicts, which can be considered a form of intelligence. In his speech at the Russian Academy of Sciences in March 2019, Gerasimov (Krasnaya Zvezda, 2019) again stressed the importance of considering modern warfare as consisting of military and non-military means of war, and the importance of achieving surprise. He also highlighted the importance of preventive measures, the identification of vulnerabilities, the importance of creating deterrence, and maintaining the ability to take strategic initiative.

According to Bērziņš (2014, 3), Russia's military strategy is based on three interrelated doctrinal levels: unilateralism, strong legitimacy, and the systematic denial of the use of military force. In this context, scholarly unilateralism refers to the idea that legitimacy could be derived from the successful use of force, while respect for legality refers to Moscow's attempts to base its actions on some "legal" grounds. The ban on the use of open military force can be better understood in the light of Russian diplomatic rhetoric in Crimea. Instead, in evaluating recent strategic communications by the Russian military leadership, the ban on open military force has somewhat receded. Given the events in the Kerch Strait, the credibility of communications has been strengthened through the use of legitimately justified military force.

The Russian Information Security Doctrine (2016, 3-6) states that the use of cyber methods and the need to protect against them are clear. The doctrine defines Russia's national interests in the information space to include maintaining continuous and smooth information operations on the information infrastructure, especially in the case of Russia's critical information infrastructure and the Russian integrated telecommunications network in the case of a direct aggressive threat and during the war. The doctrine also emphasizes geopolitical interests, the information infrastructure for military purposes, and the intelligence and psychological tools used by intelligence services to undermine internal political and social situations in different regions of the world. The Russian security services are obliged by all means to act in accordance with these goals also outside state borders.

The Russian military strategy is supposed to include the goal of creating an alternative reality to the adversary's operating environment, as well as the anti-access / area-denial zones for both its own and international information space. Russia is pursuing the leadership of its forces in a common information space, but is also preparing for threats to its information space by both defensive and offensive methods, while reinforcing its own national narrative with the legitimacy of its actions and the western belief in the actualization of created threats. Kari (2019, 17) has summarized this approach to cyber threats from the Russian doctrines as follows: "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." The technical management of the cyber environment plays a major role here. Russia's technical cyber defense 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. Russia's cyber deterrence is based on active cyber defense that combines cyber defense and offensive operations. Russia's offensive cyber operations include distributed denial of service (DDoS) attacks and advanced persistent threats (APT). Russian cyber deterrence is seen as credible, because the country has capability and it has sent the right message to adversaries, for example in 2007 to Estonia and in 2008 to Georgia (Kari, 2019, 89-92).

Yet only after 2015 has legislative action to promote information security progressed relatively quickly. The most important legal reforms for digital sovereignty and cyberspace management focused on the security of critical information infrastructure, the ban on network users' anonymity, the operators' obligations to store message and call content (the so-called Yarovaja package). The new legislation gave also

measures and obligations to build its own sovereign information network (the RUNET), which can be detached from the global data network as needed.

These legislative packages empowered, among other things, the Russian Federal Technical and Export Control Authority to issue precise regulations on hardware, software, standards, and operating processes, as well as on operators considered to be subject to critical infrastructure regulations. In addition, unrestricted access to messages for Russian security services and other security authorities was authorized, along with access to encrypted communications that telecommunications operators and other communications service providers are required to record.

In April 2019, the Russian House of Commons also approved a bill on the RUNET that obliges Russian telecom operators to ensure that RUNET is available without connection to the rest of the Internet and that all communications are routed through nodes approved or controlled by Roskomnazor. The RUNET legislation aims to ensure national information security in Russia, manage network operators and acceptable content, and reduce the traffic and security risks related to transboundary traffic (Kukkola & Ristolainen, 2019, 74-78).

Permanent war against Russian digital sovereignty is waged every day (Sinovets, 2016). The USA has been conducting cyberspace exploitation in Russian power grid systems since 2012 and prepared cyber-attacks by installing malware in the Russian information infrastructure. One threat to Russia in cyberspace is the technological gap between the Russian Federation and the leading foreign states in information and communication technology (ICT). This gap limits Russia's capabilities to respond to cyber threats (UP-646, 2016) – to resort, in other words, to deterrence by punishment.

Russian cyber deterrence by denial can be explained by the factors and elements of Russian strategic culture. The factors influencing Russian strategic culture, such as a sense of vulnerability, fear of surprise attack and invasion, the narrative of Russia as a besieged fortress and the concept of permanent war, influence Russian strategic culture in cyberspace as well. One of the basic assumptions of Russian strategic culture is that the world, including cyberspace, is a dangerous and volatile battlefield, where Russia has to fight every day for its digital sovereignty (Sinovets, 2016). The National Security Strategy of the Russian Federation (UP-683, 2015) states that the use of force in international politics is increasing. Historical experiences have created a sense of vulnerability and the fear of invasion within Russian strategic culture (Cimbala, 2013). Geography, too, has an influence. The country's lack of natural borders has created a sense of vulnerability and the need for a buffer zone, political and military control of neighboring spaces, and territorial expansion to natural, easily defensible borders (Ermarth, 2006). Russia's technological inferiority and its backwardness in the development of high technology also has an influence on the country's strategic culture. This means that Russia must be prepared for a surprise attack by a technologically superior enemy. The best option is deterrence by denial.

## 5. Conclusions

Russia has created an active cyber deterrent through both psychological and technical methods. In its strategic documents Russia has created a comprehensive picture of cyber threats and the need to protect against them. At the same time, the Russian military leadership has been actively communicating the importance of asymmetric methods of warfare and the need to increase the country's capabilities in this area.

As regards the emphasis on the development and use of cyber capabilities, Russia has moved in a more operational direction in its strategic communications, which may indicate an improvement in cyber capabilities and require the armed forces to use them more widely and for a variety of purposes. The Russian Military Doctrine creates cyber deterrence by demonstrating a readiness to defend against cyber operations, using conventional force when needed, though the use of nuclear weapons is reserved as a defense mechanism only against conventional attacks.

Technically dominating a well-controlled information space such as the RUNET opens up many opportunities for Russia to create an active cyber deterrent. First, the RUNET provides a (theoretically) defined and controllable space to be attacked and defended. Second, the lockable cyber domain allows for a variety of offensive capabilities to be developed and tested more secretly than they would be in the global information space. Thirdly, the RUNET can also attract states or other actors close to Russia to use it and thereby strengthen the creation of a common entanglement deterrence. 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.

Russia's psychological and technical measures to create cyber deterrence clearly illustrate the impact of Russia's strategic culture and the accompanying need to reinforce the narrative of Russia as a besieged and threatened fortress. They also reflect Russia's approach to adopting various deterrent strategies and applying them flexibly as the case requires.

However, the existence of cyber deterrence and the desire to use cyber abilities are still largely a matter of faith for adversaries. States know that they and their critical functions are being attacked, but uncertainty about the attackers and their motives, as well as the Western interpretation of international law, act as a deterrent to responding to the attack other than by stable defensive means.

We have previously discussed how Russia creates cyber-deterrence. Russia's way of creating a cyber-deterrent is not commensurate with the West (NATO) because NATO is made up of different countries with different legal, political, geopolitical and religious views. Russia has only one view at a time.

References

Bērziņš J. (2014) Russia's New Generation Warfare in Ukraine. From Implications for Latvian Defence Forces. National Defence Academy of Latvia Center for Security and Strategic Research, 2014, p.3-4. ( https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf)

Bērziņš J. (2019) Not 'Hybrid' but New Generation Warfare. From Russia`s military strategy and doctrine. Howard G. E. and Czekaj, M. (Eds.) (https://jamestown.org/wp-content/uploads/2019/02/Russias-Military-Strategy-and-Doctrine-web.pdf?x29008&x87069), pp. 157-184

Chekinov, S. G. and Bogdanov, S. A (2012) "Initial Periods of War and Their Impact on a country's Preparations for a Future War," Voennaya Mysl' (Military Thought), No. 11 2012, pp. 14-27

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)

Denning, D. E. (2013): Framework and Principles for Active Cyber Defense. http://hdl.handle.net/10945/59868

Denning D.E and Strawser B.J (2017) Active Cyber Defense: Applying Air Defense to the Cyber Domain. From Understanding Cyber Conflict: Fourteen Analogies Perkovich G. and Levite A.E. (Eds) Published by Georgetown University Press (https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_Ch12.pdf)

Ermarth, F. 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)

Goodman, W. (2010) Cyber Deterrence Tougher in Theory than in Practice? Strategic Studies Quarterly - Fall (https://apps.dtic.mil/dtic/tr/fulltext/u2/a528033.pdf)

Hathaway M. E. & Klimburg A. (2012)Preliminary considerations: On national cyber security. From National cyber security framework manual. Edited by Klimburg, A. NATO Cooperative Cyber Defence Centre of Excellence. (https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf) pp.1-43

Jasper, S. (2018) U.S. Strategic Cyber Deterrence Options. (http://centaur.reading.ac.uk/79976/1/22839264_Jasper_thesis.pdf)

Jasper, S. (2017) Strategic cyber deterrence. The active cyber defence option. Rowman & Littlefield Publishers. London.

JP 3-0 (2017) Joint Publication 3-0 Joint Operations 17 January 2017 Incorporating Change 1 22 October 2018 (https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910)

Kari, M. J (2019) Russian Strategic Culture in Cyberspace Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats. JYU DISSERTATIONS 122

Kello L. (2014): The Virtual Weapon: Dilemmas and Future Scenarios. in Politique étrangère 2014/4 (Winter Issue) Pages 139 – 150 (https://www.cairn-int.info/article.php?ID_ARTICLE=E_PE_144_0139)

Krasnaya Zvezda (4.3.2019) Векторы развития военной стратегии. (http://redstar.ru/vektory-razvitiya-voennoj-strategii/)

Komsomolskaya Pravda (26.12.2017) Начальник Генштаба Вооруженных сил России генерал армии Валерий Герасимов: «Мы переломили хребет ударным силам терроризма» (http://archive.redstar.ru/index.php/component/k2/item/35551-my-perelomili-khrebet-udarnym-silam-terrorizma)

Kukkola J. – Ristolainen M. (2019) Projected Territoriality: A Case Study of the Infrastructure of Russian Digital Borders. In: GAME PLAYER. Facing the structural transformation of cyberspace. Kukkola & all (Eds.). Puolustusvoimien tutkimuslaitos. Julkaisuja 11. Riihimäki 2019, pp.65-89

Manjikian, M. 2016: Deterring cybertrespass and securing cyberspace: Lessons from United States from border control strategies. (https://publications.armywarcollege.edu/pubs/2401.pdf)

Mandel, R. (2017) Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks. Georgetown University Press.

McCulloh T. and Johnson R. (2013): Hybrid Warfare. https://jsou.socom.mil

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

Nye J. S. Jr (2017): Deterrence and Dissuasion in Cyberspace. International Security, Vol. 41, No. 3 (Winter 2016/17), pp. 44–71 (www.mitpressjournals.org › pdf › ISEC_a_00266)

Pescatore, J. & Sager, T. (2013) Critical Security Controls Survey: Moving From Awareness to Action June 2013. SANS Whitepaper. (https://slidelegend.com/queue/sans-2013-critical-security-controls-survey-moving-sans-institute_59d017541723dd3afea35be0.html)

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)

Ryan, N J (2018) Five Kinds of Cyber Deterrence. Philosophy & Technology. September 2018, Volume 31, Issue 3, pp 331–338. (https://link.springer.com/article/10.1007/s13347-016-0251-1#Sec1)

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)

Sinovets, P (2016) '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

UP-683, 2015. Russian National Security Strategy. (http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf)

The Doctrine of Information Security of the Russian Federation 2016 (http://www.mid.ru/en/foreign_policy/official_documents/asset_publisher/CptICkB6BZ29/content/id/2563163)