The Cumulative Cyber Deterrence

Maija Turunen and Martti J. Kari
Finnish National Defence University,Finland
University of Jyväskylä, Finland
maijaturunen@yahoo.fi
martti.j.kari@jyu.fi

Abstract: The cumulative cyber deterrence can be seen as a concept in which increasing the weight of different means and their use increases the deterrent effect on a common level or on selected adversaries. Cumulative cyber deterrence may include all traditional options of deterrence, and can be active or passive. Active deterrence can be characterized as targeting specific threats and actors, as a deterrent consisting of several different methods, while passive deterrence is a form of deterrence commonly targeted at all the potential adversaries. The cumulative cyber deterrence can be an independent type of deterrence or part of a state's overall deterrence. This paper approaches the concept of cumulative cyber deterrence from a military perspective. The purpose is to determine what factors can be formed by cumulative cyber deterrence. It describes how cumulative deterrence will change and be affected and what problems can be associated with that concept. The aim is to find answers to these questions by looking at the way how Israel and Russia use cumulative cyber deterrence as part of their overall deterrence. In its theoretical context, this paper is based on the theory of the character of war. Through the theory of character of war and utilizing the concept of reflexive control, an attempt is made to explain the position of cumulative cyber deterrence as part of overall deterrence. Integrative literature analysis has been used as the research method. The key conclusion of the paper is that creating a credible cyber deterrent is an affect and cost-effective way to increase overall deterrence. However, this presupposes that the state also has offensive cyber methods at its disposal and is able to credibly communicate their existence and the will to use them if necessary. The concept of cumulative cyber deterrence depends on the other means of deterrence available to the state. Both Israel and Russia have all these qualities. A key difference in the deterrence strategies of these states is that Israel uses cumulative methods to make it clear where the red lines are, while Russia's strategic goal is to blur them.

Keywords: Cyber Deterrence, Russia, Israel, Red Lines

1. Introduction

Cyberspace is a dynamic, aggregated and rapidly changing battle domain with a wide range of actors and threats. The cyber deterrent may be part of the state's overall deterrence or just part of military deterrence. The cyber deterrent may be targeted solely against attacks in the cyber domain, or it may include a punitive element against hostile acts in other domains as well.

An overall deterrence or restraint created by the state can consist of a combination of political, military, informational, diplomatic, financial, intelligence, economic, legal, and developmental methods and measures. The use of cyber measures is generally considered a military, intelligence or information method, even though the objectives may be, for example, political or diplomatic. In this paper, cyber methods are discussed as part of overall military deterrence. The hypothetical question is if cyber methods can create an detached deterrent that is independent from other forces or weapon systems, for example, if an adversary is led to believe that someone has access to its C2ISR (Command, Control, Intelligence, Surveillance, Reconnaissance) systems and hostile behavior will result in punishment in those systems.

In the cyber warfare, the targets of operations can be varied: attacking the information available to the adversary, blurring the situational awareness and perception of the war character; interfering with or paralyzing the operation of the adversary's command, control, surveillance and weapon systems; obstructing or impeding the use of the adversary's critical infrastructure; (Arquilla & Ronfeld, 1993, 31, 33) creating an anti-access/area denial (A2/AD) battle domain and/or creating access to an adversary's A2/AD mode, and so on. In the concept of cumulative cyber deterrence, these targets can be valued and the force used for countermeasures adjusted accordingly.

The authors consider that cyber deterrence can be seen as consisting of the strategic, operational, tactical and technological capabilities of the state or its allies, the ability to develop them, the credible communication of their existence and the willingness to use them when necessary. These capabilities, the principles of use them, and targets vary at different levels. The state can strategically communicate its cyber deterrence through, for example, statements from its political or military leadership (will), strategy papers, legislation (plans), military exercises or even its operations (capability).

When acting at the operational level, the deterrent can be controlled using defensive, offensive or command and control system operations or, more specifically and especially in connection with deterrence, flexible defence operations (FDO) and flexible response operations (FRO). They both provide the ability to scale up (escalate) or de-escalate based on continuous assessment of an adversary's actions and reaction (JP 3-0, 2017, VIII-9). U.S. Department of Defense Science Board (2017, 15) highlights the importance to maintain scalable offensive cyber capabilities as an integral part of its cyber deterrence posture. This requires the credibility and explainability of cyber counterattacks and responses. On the operational level, the timing and operational complexity of cyber operations are emphasized (Schulze, 2020, 193).

The tactical level capabilities like operations control- and execution are typically unique and the use of the force and cyber methods by situation based. The problem with using tactical level capabilities is that they can usually only be used once (Schulze, 2020, 192). The existence, or lack thereof, of technical capabilities is well suited to the clandestine and covert world of cyber influencing. One way to get information about technological capabilities is analyzing completed operations or something about the potential capabilities of a state can be deduced by analyzing its cooperative and alliance relations.

1.1 Theoretical background and research methodology

This research applies the theory of the character of war to cumulative cyber deterrence. The character of war can be defined as the perceptions in the international system of the nature, needs and possibilities of the use of armed forces, as well as the effective principles and operating models of the armed forces (Raitasalo et al, 2008, 9). The use of the concept of reflexive control seeks to influence the adversary's situational awareness and, more broadly, the perception of the character of war. The concept of reflexive control has been designed to be executed at strategic, operational, and tactical levels (Kasapoglu, 2015, 5).

The concept of reflexive control consists of analyzing an adversary's behavior, ideas and practices and then trying to influence them. Reflexivity refers to the creation of a particular pattern of behavior in a system that is sought to be influenced and controlled (the objective system). It takes into account the fact that the object system has a situation picture that is also assumed to affect the adversary's leadership or sociopolitical system. Reflexive control utilizes moral, psychological, and other factors as well as the personal qualities of leaders. The concept of reflexive control can be seen as creating a framework for action aimed at influencing the action of an adversary so that it voluntarily begins to act in the desired way (Thomas, 2004, 237–242).

The concept of reflexive control plays a central role in Russian art of warfare, which is also influenced by strategic culture. Kari (2019, 71; Johnston, 1995) explains strategic culture as a set of persistent and consistent historical patterns of how state leadership thinks about the use of force to achieve political goals. The preferences originate in the historical experiences related to the threat and use of force by the state and are influenced by the philosophical, political, cultural, and cognitive experiences and characteristics of the state.

Integrative literature analysis has been used as the research method. By integrating and analyzing the literature on deterrence in general and cyber deterrence in particular around the research question "Cumulative Cyber Deterrence", the aim is to position the examination of the research question as part of the scientific debate on the topic.

2. The Concept of Cyber Deterrence

The concept of cyber deterrence has been discussed in the literature: can it be an independent deterrent, part of another deterrent or does it exist at all? According to Soesanto and Smeets (2020, 392-394), views on this issue can be roughly divided into three groups: (1) cyber deterrence functions akin to conventional deterrence; (2) cyber deterrence features as unique issues because cyberspace is markedly different from the traditional domains; and (3) cyber deterrence is impossible.

Analyzing these views, the authors estimated that the cyber deterrent in its objectives corresponds to a conventional deterrent. 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 adversary's 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). Furthermore, 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."

Compared to land, air, sea, and space domains, the cyber domain is different, because changes there can occur very fast and comes unnoticed. There are more potential adversaries and the cyber weapons they use may be unknown. It is precisely because of this constant activity in cyberspace and its rapid pace of change, for example, that Williams (2017) is skeptical of the deterrent's functionality in cyberspace as an operational environment because he sees an absence of action as an indication of deterrent effectiveness. Instead Nye (2016, 46) writes, "The term 'cyber deterrence' can be confusing because theorists tend to focus on in-kind or in-domain deterrence rather than on a broad range of tools that can be used both actively and passively and with graduated effects." Denning (2015, 11–15) sees the concept of cyber deterrence as problematic because it is so broad. According to Denning, one possible approach is to focus on classes of cyber-weapons and activities in cyberspace.

If we think that cyber-attacks are always aimed directly at information and indirectly at users of information, one can agree with Nye's views: weapon systems in all types of weapons and their users need the right information. By blocking (from people or weapons) access to this information or making it unreliable, it is possible to influence from cyber domain to the other domains. As with other domains, it is possible to influence a cyber domain, for example, by destroying parts of psycho-physical layer.

Tor (2015, 107–108) has listed five basic principles of the cumulative deterrence paradigm that must be adapted to the cyber domain. They are as follows:

- A strategic message regarding the 'red lines' of the deterring party;
- An ability and willingness to carry out attacks on rivals, and to set a 'price tag' on cyberattacks;
- An ability and willingness to threaten and demonstrate capabilities both in cyber and through military tools or through diplomatic and financial tools;
- Overwhelming supremacy in cyberspace; and
- The effort to build a more robust and secure cyber infrastructure through constant development of technology and protection methods.

Achieving overwhelming supremacy in cyberspace is quite unrealistic due to the complexity of cyberspace (JP-12, 2018, I-2). Maintaining local, demarcated A2/AD zones can also be a challenge, although Russia, for example, is pursuing this with its RuNet program (Kukkola, 2020).

There are also problems with setting a red line and its credible defence, for example, in the clear communication of its existence and the consequences of its violation. The adversary may also rush to test the extent of the red line or try to stretch its boundaries by hybrid methods. Libicki (2012, 68) discusses about "salami tactics", by which he means that once a state tolerates small violations, the cumulative effect begins to pinch, and the state realizes that it has neglected to establish a clear line to demarcate tolerable from intolerable violations and that can lead to an unpredictable set of results. Freedman (2020, 9) argues that: "Deterrence works best with unambiguous red lines, established over time, linked with vital interests, and backed by clear and credible messages, reinforced by known capabilities, about what will happen if they are crossed." Hybrid influence, and cyber operations as part of it, is precisely a matter of testing the red lines of an adversary, creating uncertainty in political or official decision-making or applications of law, and thus the possibility of using military retaliation.

Challenges related to the build of cumulative cyber deterrence include, for example, its credibility, the communication of the cost of the attack, psychological influence on the adversary, and problems of manipulation and regulation. A credible cumulative cyber deterrent requires that the attack is also responded to or retaliated against. Bradly (2018, 45) argues that most retaliations are not feasible in cyberspace because they require the identification of the perpetrator, retaliation within a proximate temporal range, and proportionality while a state must also possess a specific cyber weapon system tailored to its target.

3. The Cumulative cyber deterrence in the military concepts of Russia and Israel

3.1 Russia

In the Russian philosophy of warfare, concealment and deception play an important role. General Gerasimov, the chief of staff of the Russian armed forces, has stressed (Krasnaya Zvezda, 4 March 2019) the importance of

considering modern warfare as consisting of military and non-military means of war, along with the achievement of surprise. He also highlighted the importance of preventive measures, the identification of vulnerabilities, creating deterrence, and maintaining the ability to take strategic initiative.

Russian Deputy Prime Minister Dmitry Rogozin (Rogozin, 2013) said already in 2013 that enemy can paralyze critical infrastructure of a target state with cyber-attacks). According to Russian experts Stuxnet was the first example of the cyber warfare and such an attack on Russian targets could cause enormous damage to Russia's economy (Orlov, 2011).

Putin has stated that the Soviet Union was a besieged fortress and under threat of attack from the West (Aron, 2008). As a continuation of this the Russian leadership has created a narrative according which Russia is under siege and under threat of attack from the West. The narrative that Russia is target of enemy states (Facon, 2016) and the country's perceived geostrategic and technological vulnerability (Covington, 2016), combined with Russia's feeling of a hostile world (Facon, 2017), have strengthened the Russian narrative of the besieged fortress (Igumnova, 2011). As a besieged fortress, Russia needs to be protected.

This besiege has expanded to cyberspace. According to Igor Ashmanov, a Russian ICT specialist, the cyber warfare against Russia is waged every day and no rules of war apply to it (Yarovaya, 2013). As a part of this warfare Russia has actively built its cyber deterrence. The main tasks of the Russian Federation regarding deterring and preventing military conflicts is to create conditions to reduce the risk of using information and communications technologies for military-political purposes (National Security Strategy 2021, art. 40).

Russia's way of building deterrence can be explained by the factors and elements of Russian strategic culture. The main factors influencing Russian strategic culture are its sense of vulnerability, fear of surprise attack, the narrative of Russia as a besieged fortress and the concept of permanent war. Russia is lagging behind the leading countries in the development of competitive information technology, and this gap strengthens the Russian perception of its strategic vulnerability in cyberspace. Russia's cyber deterrence consists of improved protection of its critical information infrastructure, preparations to isolate the Russian segment of the Internet from the global Internet, intensified surveillance, the ban of user anonymity on RuNet, and the aspiration to replace imported information and communication technology with Russian-produced ICT (Kari, 2019).

Russia tries to maintain the status quo or change it, not just threatening the adversary with retaliation or by denying it of its objectives through intolerable risks and costs (Kukkola, 2020, 185). Russia also shapes the strategic operating environment and manipulates its adversaries' perception while influencing its strategic behavior and using different flexible non-linear and cross-domain methods (Adamsky, 2021, 161, 170, 172).

Russia operates in the cyber environment. In addition to the cyber espionage targeted at the US Democratic Party in 2016, Russia was credited with intrusion into the e-mails of representatives of the Norwegian and Finnish parliaments in 2020, all of which Russia has actively denied. Russia has been linked to violent episodes such as that around the Bronze Soldier in Estonia in 2004, the Georgian War in 2008 and the conquest of Crimea in 2014. All these conflicts have been preceded by a cyber-attack on some socially important system in the target country. On the basis of these examples, it can be estimated that Russia and its authorities have good opportunities to control cyber-activities within its sphere of influence.

3.2 Israel

The public defense doctrine of the Israel Defense Forces (IDF, 2015), or the so-called Eizenkot's IDF Strategy, emphasizes strategic and tactical deterrence via cyberwarfare (Frei, 2020, 9). The strategy notes that deterrence against any enemy must be generalized and cumulative over time in order to maintain the existing situation and frame "rules of the game" favorable to Israel. Israel's Cyber Security Strategy (2017) also highlights to importance of operations and active efforts to confront the sources of the threats. The concept of operations defines three operational layers: Aggregate Cyber Robustness, Systemic Cyber Resilience and National Cyber Defense.

The development of capabilities and building up forces are based on strengthening strategic and tactical deterrence via cyber warfare (Belfer Center, 2016, 24, 48). Tor (2015, 111–112) argues that the cumulative deterrence theory developed in Israel in a conventional strategic context. Deterrence is perceived as a spectrum rather than a dichotomous, binary state. "The cumulative deterrence paradigm considers sporadic, short bursts

of violence as an integral part of a 'learning process' between the opposing parties. Such intermittent strategic interactions are meant to lead the deterred party to understand the 'red lines' of the deterring party."

Israel's concept of cumulative cyber deterrence is in nature deterrence by punishment. That includes limited and designed deterrence and influence operations, which are typically combined with a limited use of conventional force. The purpose of the operations is to reinforce the deterrent by trying to influence the adversary's behavior and to set the rules of the game for hostile interaction (Tor, 2015, 105–107). According Almog (2004, 3, 6), classical deterrence and cumulative deterrence differs from conceptualization and implementation to desired results. On the macro level, cumulative deterrence seeks to create an image of overwhelming military supremacy and on the micro level, it relies on specific military responses to specific threats or hostile acts.

Maintaining deterrence and its credibility requires constant renewal. This means that the response to attacks should be immediate, certain, and the amount of force properly calibrated to the attack (Almog, 2004, 6; Shamir, 2020, 275, 276). Iran and Hamas have often been behind the significant public cyber-attacks against Israel. Israel has retaliated against the attacks in, for example, the 2010 Stuxnet attack against Iran's nuclear power plant and the retaliation in 2019 for Hamas's offensive cyber-attacks they bombed a Hamas cyber center (Frei, 2020, 6).

In assessing the concept of Israel's cumulative cyber deterrence, it is good to take into account geopolitical, political, historical, cultural, and diplomatic considerations. A similar concept that flexibly combines cyber and conventional methods of using force would not necessarily work in the Western countries. First, the use of military force has been a part of "everyday life" (on their own soil and borders) and a necessary activity throughout Israel's history due to its location and the presence of a hostile minority. Second, in no way is, from the point of view of the actors in the area referred to above, the use of military force in any way surprising or exceptional, but part of an ongoing conflict. Third, Israel's strong alliance with the United States helps strengthen the legitimacy of its actions from the perspective of international law. Thus, it can be estimated that Israel's cumulative cyber deterrence alone does not work, but contributes to strengthening Israel's overall deterrence. The problem with the Israeli concept of cumulative cyber deterrence is that while they seek to draw red lines and respond to the crossing of them with conventional force if necessary, the adversary nonetheless seeks to defy their defenses over and over again. It is no longer a question of the effects of cyber deterrence or its failure, but of the state of mind of the adversary.

4. Conclusions

The cumulative cyber deterrence in order to operate independently requires a limited and defined cyber environment, one that is either formed in the operating environment of the deterrent creator A2/AD or alternatively to access an adversary's A2/AD. Second, in order to function as their own deterrent system, building a cyber deterrent requires a large number of different cyber weapons and attack methods because they are disposable against the same adversary. However, due to the uniqueness of the cyber environment as a combat domain, the diversity of change factors, it may be more realistic to see the cumulative cyber deterrence as part of the overall deterrence of states.

The cyber deterrence can be seen as consisting of the strategical, operational, tactical and technological capabilities of the state or its allies. The cumulative cyber deterrence presupposes that its existence, means, and the will to implement it have been credibly communicated through either open or tacit strategic communication to the deterrent object, without the deterrent object receiving information that can circumvent the methods that maintain the deterrent. Second, the functioning of cyber deterrence as an independent concept requires that the adversary does not have significant conventional weapons available or has no will (e.g. political or legal or technological barriers) to use them.

The comparison between the cumulative cyber deterrence concepts of Russia and Israel showed that Russia has the time and resources to wait, shape the cyber domain and signal potential adversaries about consequences. Israel's concept of cumulative deterrence is more straightforward and emphasizes the need for an immediate and credible answer. Israel's strategic deterrence can be described as deterrence by retaliation, while Russia's strategic deterrence, especially its cyber deterrence, is more deterrence by denial in nature, although the means they use are often offensive.

The concept of cumulative cyber deterrence depends on the other means of deterrence (political and military will, plans, conventional military capabilities, technological skills) available to the state. Both Israel and Russia have all these qualities. There are several similarities in the military thinking based on strategic culture behind the defense doctrines of Russia and Israel. In particular, the perception of an ongoing and permanent war in the cyber domain distinguishes these states and their concept of cumulative deterrence from "Western" states. The overall deterrence strategy of these states is based on their strategic culture and their perception of threats, which differ from each other. A key difference in the deterrence strategies of these states is that Israel uses cumulative methods to make it clear where the red lines go, while Russia's strategic goal is to blur them and create the fog of war.

In the scope of the future, it is obvious that both Israel and Russia are investing in the development of artificial intelligence, robotics and autonomous weapon systems. Success in this development is likely to reinforce deterrence, but on the other hand, this also highlights the importance of cyber defense: advanced weapons systems can be also unpredictable and vulnerable.

References

Adamsky, D. (2021) Deterrence à la Ruse: Its Uniqueness, Sources and Implications. F. Osinga and T. Sweijs (eds.), NL ARMS Netherlands Annual Review of Military Studies 2020, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_9. pp.161-175.

Almog, D. (2004) Cumulative Deterrence and the War on Terrorism .United States Army War College Quarterly (Winter 2004-05), v.34 no.4, p.4-19. https://www.hsdl.org/?view&did=453973.

Aron, L. (2008) 'The Problematic Pages. In memory of Alexander Solzhenitsyn', The New Republic. (24 September 2008). https://newrepublic.com/article/62070/the-problematic-pages.

Arquilla, J. & Ronfeld, D. (1993) Cyberwar is coming! https://www.rand.org/pubs/reprints/RP223.html.

Belfer Center for Science and International Affairs (2016) Deterring Terror. How Israel Confronts the Next Generation of Threats. English Translation of the Official Strategy of the Israel Defense Forces Foreword by Graham Allison. https://www.belfercenter.org/sites/default/files/legacy/files/IDFDoctrineTranslation.pdf.

Brantly, A. (2018). The cyber deterrence problem. In T. Minárik, R. Jakschis, & L. Lindström (Eds.), *10th international conference on cyber conflict.* Tallinn: NATO CCD COE Publications. Retrieved from: https://ccdcoe.org/uploads/2018/10/Art-02-The-Cyber-Deterrence-Problem.pdf.

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

Denning, D.E. (2015) Rethinking the Cyber Domain and Deterrence. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_8-15_Denning.pdf.

Department of Defense Science Board (2017) Task Force on Cyber Deterrence. https://www.hsdl.org/?collection&id=2724.

Facon, I. (2016) '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, 62-89. http://nbr.org/publications/strategic_asia/pdf/SA16_ExecutiveBrief.pdf.

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

Freedman, L. (2020) Introduction—The Evolution of Deterrence Strategy and Research. In Osinga, F. and Sweijs, T. (Eds.): Deterrence in the 21st Century—Insights from Theory and Practice. NL ARMS Netherlands. Annual Review of Military Studies 2020. https://link.springer.com/content/pdf/10.1007%2F978-94-6265-419-8.pdf. pp.1-10.

Frei, J. (2020) Israel`s National Cybersecurity and Cyberdefence Posture. Policy and Organizations. css.ethz.ch/en/publicatios/risk-and-resilience-reports.html.

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

State of Israel (2017) Israel National Cyber Security Strategy in Brief. https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.

Johnston, A. (1995). Cultural Realism: Strategic Culture and Grand Strategy in Chinese History. Princeton University Press 1995.

Joint Chief of Staff (2018) JP 3-0, Joint Operations. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910.

Joint Chief of Staff (2018) JP-3-12, Cyberspace Operations. https://irp.fas.org/doddir/dod/jp3_12.pdf.

Igumnova, L. (2011) 'Russia's Strategic Culture Between American and European Worldviews', The Journal of Slavic Military Studies, Volume 24. doi: 10.1080/13518046.2011.572729.

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.

Kasapoglu, C. (2015) Russia`s Renewed Military Thinking: Non-Linear Warfare and Reflexive Control. NATO Defence College, Rome – No. 121. https://cco.ndu.edu/Portals/96/Documents/Articles/russia's%20renewed%20Military%20Thinking.pdf.

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

Kukkola, J. (2020) Digital Soviet Union. The Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas. National Defence University. Series 1: Research Publications No. 40. https://www.doria.fi/bitstream/handle/10024/177157/Kukkola_Digital%20Soviet%20Union_finalnet.pdf?sequence=3&isAllowed=y.

Libicki, M. C. (2012) Crisis and escalation in cyberspace. (Santa Monica: RAND Corporation) https://www.rand.org/pubs/monographs/MG1215.html.

Nye, J. S. Jr. (2016): Deterrence and Dissuasion in Cyberspace. Quarterly Journal: International Security 2016/17) pp.44-71 https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00266.pdf.

Orlov, V. (2011) Start of new battles, Moskovskie Novosti. (21 April 2011). http://www.mn.ru/newspaper/world/68636.

Raitasalo, J. – Sipilä, J. (2008) ”Näkökulmia sotaan” Sota – teoria ja todellisuus. Näkökulmia sodan muutokseen. pp. 1-10. http://urn.fi/URN:ISBN:978-951-25-1894-4.

Rogozin, D. (2013) Speech by Dmitry Rogozin at a press conference in the "RG" (28 June 2013). (in Russian) https://rg.ru/2013/06/28/doklad.html.

Shamir, E. (2020) Deterring Violent Non-state Actors, 263-286. In Osinga, F. and Sweijs, T. (Eds.): Deterrence in the 21st Century—Insights from Theory and Practice. NL ARMS Netherlands. Annual Review of Military Studies 2020. https://link.springer.com/content/pdf/10.1007%2F978-94-6265-419-8.pdf. pp. 263-286.

Schulze, M. (2020) Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations https://ccdcoe.org/uploads/2020/05/CyCon_2020_10_Schulze.pdf.

Soesanto, S. and Smeets, M. (2020) Cyber Deterrence: The Past, Present, and Future. In Deterrence in the 21st Century—Insights from Theory and Practice. Annual Review of Military Studies 2020. pp. 386-397 https://link.springer.com/content/pdf/10.1007%2F978-94-6265-419-8.pdf.

Thomas, T. (2004) Russia’s Reflexive Control. Theory and the Military. Journal of Slavic Military Studies 17: 237–256. https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf.

Tor, U. (2015) Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence. December 2015Journal of Strategic Studies 40(1-2):1-26Williams, B. D. (2017) Meet the scholar challenging the cyber deterrence paradigm. https://www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/.

Yarovaya, M. (2013) ‘Igor Ashmanov: ‘Today information domination is the same as air superiority’’, https://ain.ua/2013/05/01/igor-ashmanov-segodnya-informacionnoe-dominirovanie-eto-vse-ravno-chto-gospodstvo-v-vozduxe.