Options for Signalling Cyber Deterrence Using Cyber Capabilities

Maria Keinonen[1] and Kimmo Halunen[1,2]
[1]National Defence University, Helsinki, Finland
[2] University of Oulu, Oulu, Finland

maria.keinonen@mil.fi
kimmo.halunen@oulu.fi

Abstract: The possibility of demonstrating power in cyberspace to create deterrence is a controversial topic. The desire of states to hide their true cyber capabilities leads to a reluctance to reveal their existing cyber power. However, the core idea of deterrence involves demonstrating power and signalling the will to use it so that the potential aggressor would find it less tempting to carry out aggression. Several studies attempt to solve the challenges related to cyber deterrence with a holistic approach, where deterrence in cyberspace is produced as part of a comprehensive deterrence using all instruments of state power, such as diplomatic, information, military, economic and legal capabilities. In turn, some studies argue that for credibility, cyber deterrence must include measures implemented specifically in cyberspace because cyberattacks can only be responded to in real-time with cyber capabilities. This paper argues that demonstrating cyber power is both necessary and profitable for the credibility of deterrence, although the nature of cyberspace and related technologies pose some limitations. This study examines the possibilities of demonstrating cyber power in concrete ways and aims to add a new perspective to academic debate. Cyber deterrence is investigated from the perspective of classical deterrence theory, including deterrence by denial and deterrence by punishment. By examining cyber deterrence literature using content analysis, deterrents that can be produced with cyber capabilities are defined, and examples of means to produce these effects are presented. According to the central observation of the study, a state can choose whether to demonstrate cyber power by revealing the victories achieved in real-life cyber battles, by demonstrating force in another state's cyberterritory or by disclosing selected capabilities in separate simulations without a real-life connection.

Keywords: Cyber deterrence, Cyber power, Cyber deterrence signalling, Demonstration of cyber power

1. Introduction

Cyber deterrence can be understood in at least three different ways. First, it can be understood as using the state's cyber power as a deterrent against a military attack. The second conception is using military resources as a deterrent against a cyberattack. Third, it may mean using the state's cyber capabilities as a deterrent against a cyberattack. (Soesanto & Smeets, 2021) This paper investigates the third option from the perspective of deterrence signalling.

Cyber deterrence research is focused on controlling real-life cyber events and demonstrating power with cyber operations (Bendiek & Metzger, 2015). Only a few studies focus on the enablers of cyber operations, such as governance, training and decision-making (Huskaj, 2019). Also, displaying cyber power that does not involve real-life cyber operations has received less attention. This research explores the possibilities of demonstrating cyber power in real-life events and other ways that do not require the disclosure of the state's critical cyber capabilities.

Due to the unique characteristics of cyberspace, there are still many unsolved challenges associated with cyber deterrence. Some of these challenges could be resolved with already existing implementation options if consciously combined with deterrence signalling. These options are investigated in this article. The research question is: *"What kind of options can be utilised for cyber deterrence signalling?"* To answer the question, the study analyses cyber deterrence literature and forms an understanding of the possibilities and limitations of cyber deterrence signalling. This analysis sets the conditions for solutions sought from real-life cyber events as examples of how cyber deterrence can be signalled.

2. Theoretical Background

At the core of the classical deterrence theory is the idea of force, which the state is ready to use against aggressions by other states. The will to use this force is communicated preventively to decrease the threat actor's desire to behave aggressively. With the changing power relations in world politics and the development of cyberspace, the need for deterrence has remained. However, the concept has changed from absolute nuclear deterrence to a broad spectrum of deterrents and flexible escalation control. (Freedman, 2021)

A fundamental dichotomy in classical deterrence literature appears in subsequent deterrence studies in one form or another. According to these studies, deterrence can be divided into deterrence by denial and deterrence by punishment. The goal of deterrence by denial is to convince the threat actor that aggression will

not achieve the desired effects and goals. The main message of deterrence by punishment is that at least an equal response follows that aggression. The classical deterrence theory assumes that deterrence is implemented by states that signal their intentions to each other. Deterrence will then fail if aggressions are carried out. (Mazarr, 2021)

The principles of classical deterrence theory do not apply to cyberspace as such (Taddeo, 2018), and it is no longer a dichotomous concept where it either succeeds or fails depending on the aggressions that have taken place (Chen, 2023). Cyberspace will not achieve complete immunity from attacks because it offers more opportunities for attack than opportunities for protection. (Tor, 2017) However, this is not a valid reason not to engage in deterrence signalling related to the protection of cyberspace sovereignty.

Part of deterrence signalling is a demonstration of force. Warfighting is the state's most unambiguous opportunity to demonstrate its military power. Since deterrence aims to prevent aggression, force must be demonstrated before tensions escalate into an armed conflict. In peacetime, states can demonstrate their military power with military exercises and deliberately promote experiments and exhibitions. These means can also be used for abilities that are more difficult to demonstrate, such as cyber capabilities. (Montgomery, 2020)

The classical deterrence theory requires the ability to respond to aggression. That, in turn, requires the ability to identify the attacker reliably. In cyberspace, attribution can be challenging if techniques have been used that make it possible to hide the origin of the attack. Although the development of technology has enabled more effective attribution, the state rarely wants to report the attack to hide its actual cyber capabilities. (Lonergan & Lonergan, 2023; Chen, 2018; Taddeo, 2018; Wanic & Rowe, 2018; Lee, 2015) On the other hand, developing technology to enable attribution is profitable for the state because successful attribution also increases the credibility of cyber deterrence (Navicky & Tkach, 2023; Baliga et al., 2018; Chen, 2018). Therefore, cyber deterrence signalling via real-life actions is problematic because states want to hide their cyber capabilities. At the same time, deterrence is based on publicised facts of capability and will to use it.

Another challenge of cyber deterrence is credibility, the lack of which renders signalling useless. In contrast to nuclear weapons and conventional military power, cyber capabilities represent soft power that can hardly directly achieve massive destructive power, as required by deterrence by punishment. (Lonergan & Lonergan, 2023; Chen, 2018, Taddeo, 2018; Lee, 2015) For this reason, cyber deterrence signalling must be based on factors other than brute force.

For the challenges presented, the academic discussion on cyber deterrence still debates different implementation options (Soesanto & Smeets, 2021). Cyber persistence theory offers a novel solution to protecting a state's sovereignty in cyberspace by continuously seeking initiatives to create and maintain favourable conditions of security in cyberspace. This approach is based on principles of exploitation rather than coercion (Fischerkeller et al., 2022). Another approach is cyber diplomacy, which enhances security and stability in cyberspace via cooperation, confidence-building and the establishment of international norms. (van der Meer, 2015) Although these approaches to state cyber security differ in principle from cyber deterrence, they offer tools that can also be utilised from the perspective of cyber deterrence, for example, the ideas of initiative, continuity and cooperation.

3. Methodology and Results

This research focuses on deterrence signalling using cyber capabilities to defend the state's sovereignty in cyberspace. It should be noted, however, that deterrence signalling includes communication about the readiness to use all the instruments of the state's power to defend its sovereignty, such as diplomatic, information, military, economic and legal measures (Sweijs & Zilincik, 2021). Together with these, the demonstration of cyber power completes the entirety of the state's deterrence signalling.

The study's theoretical basis was formed by content analysis (Puusa & Juuti, 2020). Scientific research on cyber deterrence was selected as the source material and searched in abstract and citation databases Scopus and Google Scholar. The search phrases included "cyber deterrence" and "deterrence in cyberspace". These phrases were searched from the title, keywords and abstract. The period was limited between 2013 and 2023 to form an understanding of earlier research and current views on the subject. The initial search produced 209 hits.

The screening process narrowed the focus to articles about deterrence by denial, deterrence by punishment or deterrence signalling. After screening, twenty scientific studies that focused on the possibilities and limitations

of cyber deterrence and its implementation possibilities were selected as the material to be analysed. After the first analysis round, themes were formed, and the second analysis round was based on these themes. The themes were: "features of cyber deterrence", "options for demonstrating cyber power", and "deterrence options". Categories were formed under the selected themes.

Six features of cyber deterrence were defined based on the analysed material. These features are presented in Table 1. The "x" marks the information found in each article. These features apply to demonstrating both defensive and offensive cyber capabilities.

Table 1: Results of the content analysis: part 1.

	Features of cyber deterrence					
Factor **Writer**	**Continuous actions**	**Co-operation and confidence building**	**The level of secrecy is a choice**	**Attribution is a key capability**	**Need for escalation control**	**Deterrence is not absolute**
Borghard & Lonergan, 2023	x		x			x
Chen, 2023			x	x	x	
Lonergan & Lonergan, 2023		x	x			
Navicky & Tkach, 2023	x		x	x	x	
Pedersen, 2023			x	x	x	
Brown & Fazal, 2021			x			
Kostyuk, 2021			x		x	
Klimburg, 2020		x	x		x	
Montgomery, 2020			x		x	
Baram & Sommer, 2019		x	x		x	
Fischer, 2019			x	x	x	x
Baliga et al, 2018			x	x		
Chen, 2018			x	x	x	
Taddeo, 2018			x	x	x	
Wanic & Rowe, 2018		x	x	x		x
Carson & Yarhi-Milo, 2017			x		x	
Edwards et al, 2017			x	x	x	
Tor, 2017	x					x
Lee, 2015			x		x	
Lindsay, 2015			x	x	x	

Continuous cyber operations signal to the threat actor about the state's maturity to protect itself from cyberattacks, making it difficult for the threat actor to carry out the aggression. Such continuity can reduce the threat actor's desire to attack. (Borghard & Lonergan, 2023) Such deterrence signalling is based on long-term activity and demonstrating determination and force in cyberspace.

International cooperation in developing cybersecurity-related laws and norms and responding to cyberattacks together signals to the threat actor the will to solve cyber threats as an international front. (Klimburg, 2020; Wanic & Rowe, 2018) Sharing information about one's cyber capabilities can instil confidence in allies and neutral parties and increase stability with a potential threat actor. (Lonergan & Lonergan, 2023; Klimburg, 2020) Signalling these actions specifically as part of deterrence could enhance credibility.

It is not advantageous for the state to reveal too much of its cyber capabilities or activities in cyberspace, so a certain amount of secrecy is needed, for example, to protect the gained foothold in opponent systems and reconnaissance (Navicky & Tkach, 2023; Baram & Sommer, 2019). A state should not reveal anything it might

want to take advantage of later (Lonergan & Lonergan, 2023). The most risk-free option is revealing facts without connection to the state's actual cyber capabilities.

Attribution strengthens if the state continuously improves its abilities for detection and identification (Baliga et al., 2018). If the state has built a credible attribution capability and publicly informs about the identified attackers, it may be easier to justify counterattacks in the eyes of the international communities (Wanic & Rowe, 2018). Correspondingly, repeated failures to identify an attacker inevitably also lead to a weakening of deterrence (Navicky & Tkach, 2023). From a signalling point of view, attribution is a crucial capability in cyberspace.

Although cyber capabilities are considered soft measures, there could be a risk of escalation if a cyberattack is answered with a counterattack. Attacks are also accompanied by uncertainty in controlling the spread of the effects of cyberattacks. (Taddeo, 2018; Lee, 2015) Therefore, there is a need for escalation control when using offensive cyber capabilities.

The state must accept that deterrence against cyberattacks is not absolute. Even so, it is worth making the cyberattack as complex and resource-consuming as possible because it can have a deterrent effect. (Fischer, 2019; Tor, 2017) Despite this, the state must signal its determination to defend itself against cyberattacks.

During the analysis, it was found that several cyber deterrence studies have focused on real-life cyber activity. This activity can be divided into countermeasures against attacks on the state and its offensive cyber operations against another state or a display of cyber power in which the state shows its power through a third party. These categories were named real-life events and proxy events in Table 2.

A real-life event can be offensive or defensive. A fundamental choice is the level of secrecy, which is also related to escalation control. For example, while demonstrating the attribution ability, one can decide to share all the related information or only about the events and their prevention, leaving the attacker's identity undisclosed (Baram & Sommer, 2019). The latter choice can help manage the risk of escalation, primarily if the communication focuses on established evidence and events, leaving sensitive issues unaddressed (Lindsay, 2015). Accordingly, when planning and executing offensive cyber operations, the state must assess the chances of getting caught and the resulting consequences (Edwards et al., 2017) and, if caught, choose whether to deny or admit guilt or even not comment on the matter at all (Brown & Fazal, 2021). Successful cyberattacks signal the state's ability and will to use force in cyberspace but might cause escalation and inevitably reveal the intelligence's footholds in opponent systems and techniques used for the attack.

Proxy events can be, for example, the sharing of information that targets a third party. When a state detects a cyberattack, it can share related findings with the target state or participate in combating and countering the attack (Klimburg, 2020; Wanic & Rowe, 2018). Through a third party, a commercial operator or another authority, it is also possible to reveal information the state does not want to associate with, for example, military intelligence capability.

The analysis found that cyber power can also be demonstrated with simulated events. These can be used to demonstrate cyber power without risking the exposure of the state's true cyber capabilities. The aim is to demonstrate the state's maturity as a cyberspace actor, including signalling expertise, technological capabilities and cooperation. Simulated events can be, for example, national and international cyber exercises, competitions and public demonstrations, which are communicated openly (Montgomery, 2020; Wanic & Rowe, 2018).

Table 2 presents the prevalence of real-life, proxy and simulated events in demonstrating cyber power and the author's point of view on the deterrence of denial or punishment in the analysed material.

According to the analysis, the basic principle for signalling deterrence by denial in cyberspace is demonstrating the ability to withstand and repel cyberattacks. Correspondingly, deterrence by punishment is signalled by demonstrating the will and ability to attack. The purpose of demonstrating cyber power is not always to inflict damage to the opponent but also to demonstrate the state's maturity to act in cyberspace. Table 3 summarises examples related to the possibilities of demonstrating cyber power for both types of deterrence. The selected examples are existing state activities and have been investigated from the perspective of real-life, proxy and simulated events.

Table 2: Results of the content analysis, part 2

	Options for demonstrating cyber power			Deterrence options		
Factor **Writer**	Real-life events	**Proxy events**	**Simulated events**	**Denial with counter-operations or retaliation**	**Denial with resilience and defence**	**Punishment with offensive cyber operations**
Borghard & Lonergan, 2023	x			x		
Chen, 2023				x		x
Lonergan & Lonergan, 2023	x					
Navicky & Tkach, 2023	x				x	
Pedersen, 2023	x					x
Brown & Fazal, 2021	x					
Kostyuk, 2021		x			x	x
Klimburg, 2020		x				
Montgomery, 2020			x			
Baram & Sommer, 2019	x					
Fischer, 2019	x			x	x	
Baliga et al, 2018				x		
Chen, 2018					x	x
Taddeo, 2018	x				x	x
Wanic & Rowe, 2018	x	x	x	x	x	x
Carson & Yarhi-Milo, 2017	x					
Edwards et al, 2017	x					
Tor, 2017	x			x		x
Lee, 2015					x	
Lindsay, 2015	x				x	x

The purpose of the simulated event is to demonstrate the state's maturity to protect its sovereignty in cyberspace via defensive and offensive means without disclosing the actual cyber capabilities. This can be achieved via cyber exercises, competitions and other simulations in training environments such as cyber ranges. They reflect either denial or punishment, depending on the type of the event.

A cyber range includes a realistic network environment with realistic scenarios, enabling various roles and teaming, feedback for learning purposes and monitoring the trainee's actions during the exercise. (Muhammad et al., 2020) A state can utilise cyber ranges for signalling deterrence by denial or punishment by publicly disclosing information about their use.

With cyber exercises, states can demonstrate their expertise, technological capabilities and ability to cooperate with other states. Locked Shields is an international cyber exercise conducted by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE); it is defensive in nature and allows states to conduct strategic signalling. (Smeets, 2022) From the deterrence by punishment point of view, the CCDCOE's Crossed Swords exercise incorporates red teaming techniques, tools, tactics and procedures (Blumbergs et al., 2019), which can be used for demonstrating offensive capabilities. Also, hacking competitions like the Pwn2Own (Portnoy, 2010) allow governments to demonstrate offensive cyber capabilities. It is profitable for states to signal their participation and success in such competitions, even if their more detailed content cannot be published.

From the point of view of deterrence by denial, a proxy event can occur, for example, by sharing information about detected attacks against another state or aiding another state to identify and counter a cyberattack. The war in Ukraine has shown the possibility of assisting another country to defend itself through collaboration

with Western nations and technology companies (Willet, 2022). This is a valuable opportunity for the supporting country to signal its ability to execute cyber operations on the territory of another state, and vice versa, an opportunity for the defender to demonstrate its abilities to act as a host country in a multinational cyber defence operation.

Signalling the states' ability to recruit patriotic hackers for offensive cyber operations benefits deterrence by punishment as a proxy event. For example, Russia published attacking guidelines against Georgia's government websites in 2008 and successfully recruited patriotic hackers for the task (Mareš & Netolická, 2020). Another example is the voluntary organisation "IT Army of Ukraine", established by the Ukrainian government, which allows cyber experts from Ukraine and other countries to execute cyber operations (Soesanto, 2023). On the other perspective, when recruiting civilians, the level of control can be challenging to establish, and some of the effects can be detrimental to the overall operation. This could also decrease the credibility of deterrence signalling.

Isolating a state's internal network from the global Internet is an extreme example of the practical implementation of real-life deterrence by denial. Such an example is Russia's RuNet. According to the plans and outspoken rhetoric, RuNet is intended to be an autonomous network that can be taken off the Internet without affecting RuNet's internal networking (Kukkola, 2020; Kukkola, 2018). Western media have commented that Russia has successfully tested this capability (Mellor, 2022; Wakefield, 2019). Even though no evidence of this has been publicly presented, talking about it can be interpreted as Russia's cyber deterrence signalling.

An alternative strategy to deterrence by denial is investing in state resilience and cyber diplomacy. For example, the European Union actively promotes the development of the international regulatory framework and projects its normative power (Miadzvetskaya & Wessel, 2022). Resilience is developed through, among other things, disruptive technologies in building a defensive shield for the EU member states. (Osula, 2022) Communicating about resilience and cyber diplomacy also strengthens deterrence signalling.

From deterrence by punishment perspective, there are examples of cyberattacks affecting cyber and physical environments. Stuxnet, released in 2010, was used to destroy critical infrastructure related to nuclear enrichment in Iran. It was in Israel's and the United States' interests to halt Iran's nuclear program, so they executed a cyber campaign code-named "Olympic Games". (Lindsay, 2013) As a result, despite the states' motives, Iran is not yet a nuclear weapon state. Therefore, the Stuxnet may have played a role in deterrence by punishment, convincing Iran that more severe consequences might occur if the nuclear program were to proceed.

Table 3: Options for signalling cyber deterrence using cyber capabilities

Deterrence strategy / Execution option	Deterrence by Denial	Deterrence by Punishment
Simulated event	*Demonstrations of expertise, technological readiness and cooperation via cyber exercises and competitions.* Examples: Cyber Ranges, Locked Shields.	*Demonstrations of expertise, technological readiness and cooperation via cyber exercises and competitions* Examples: Crossed Swords, Cyber ranges, Pwn2Own.
Proxy event	*Information sharing of detected attacks against another state. Aiding another state to identify and counter a cyberattack. The ability to receive support.* Examples: Ukraine cyber defence collaboration.	*Information sharing of potential aggressors' networks. Offensive cyber operation with another state or targeting an enemy of another state.* Examples: IT Army of Ukraine, patriotic hackers.
Real-life event	*Publicly shared information.* Examples: RuNet, EU cyber diplomacy and resilience.	*Publicly shared information.* Examples: Stuxnet, NotPetya

NotPetya, released in 2017, was originated by Russian military intelligence targeting the Ukrainian economy by encrypting and paralysing the computer networks of Ukrainian banks, firms, and government. (Crosignani et

al., 2021) Effective punishment in cyberspace generally requires technical capabilities and an understanding of the adversary's target systems. This ability could considerably threaten a potential aggressor alongside other deterrence signalling.

4. Conclusions

This article presents three options for demonstrating cyber power: simulated, proxy and real-life events. These options were examined from the point of view of deterrence by denial and deterrence by punishment, looking for implementation examples for each option.

Simulated events, for example, cyber exercises and competitions, can demonstrate the state's ability to protect its sovereignty in cyberspace without revealing the state's actual cyber capabilities. A lack of direct connection to real-life activities can be a weak deterrence signal. However, continuous signalling could create a reputation of states' cyber maturity and benefit deterrence strategies.

Proxy events can be, for example, information sharing of detected attacks against another state and aiding another state to identify and counter a cyberattack or targeting a mutual enemy. This allows the deterring state to demonstrate its ability to collect information and operate on other states' cyber territory and the defending state to demonstrate its ability to receive assistance.

Real-life events are often more straightforward to signal from the perspective of deterrence by denial because related cyber activities can often be signalled without revealing technological details and concentrating on the achieved effects. Demonstrating offensive capabilities can be more challenging because the cyber attacker often wants to hide the attack's origin. Since the level of secrecy is often a choice, the state must consider the cost-benefit calculus when using real-life events for deterrence signalling.

In conclusion, existing options exist for demonstrating cyber power through simulated, proxy and real-life events. States need to recognise these options and use them systematically for deterrence signalling. From a signalling point of view, the presented options for demonstrating cyber power differ in signal clarity and credibility. Despite this, it is worthwhile to demonstrate cyber power in as many ways as possible because these signals can create a credible image of the state's cyber deterrence.

References

Baliga, S., Bueno De Mesquita, E. & Wolitzky, A. (2020). Deterrence with Imperfect Attribution. *American Political Science Review*, 114(4), 1155-1178. doi:10.1017/S0003055420000362.

Baram, G. and Sommer, U. (2019). Covert or not Covert: National Strategies During Cyber Conflict. *2019 11th International Conference on Cyber Conflict (CyCon),* Tallinn, Estonia, 2019, pp. 1-16, doi: 10.23919/CYCON.2019.8756682.

Bendiek, A., & Metzger, T. (2015). *Deterrence theory in the cyber-century. Lessons from a state-of the-art literature review*. Working Paper, Research Division EU/Europe, Stiftung Wissenschaft und Politik, German Institute for International and Security Affairs.

Blumbergs, B., Ottis, R. & Vaarandi, R. (2019). Crossed Swords: A Cyber Red Team Oriented Technical Exercise. *18th European Conference on Cyber Warfare and Security*, Volume 2019-July, Pages 37 – 44.

Borghard, E. & Lonergan, S. (2023). Deterrence by denial in cyberspace, *Journal of Strategic Studies*, 46:3, 534-569, DOI: 10.1080/01402390.2021.1944856.

Brown, J., & Fazal, T. (2021). #SorryNotSorry: Why states neither confirm nor deny responsibility for cyber operations. *European Journal of International Security*, 6(4), 401-417. doi:10.1017/eis.2021.18.

Carson, A. & Yarhi-Milo, K. (2017). Covert Communication: The Intelligibility and Credibility of Signaling in Secret. *Security Studies*, 26:1, 124-156, DOI: 10.1080/09636412.2017.1243921.

Chen, J. (2023). Deterrence in Cyberspace: An Essential Component in Integrated Deterrence. In Billingsley, J. (ed), *Integrated Deterrence and Cyberspace, Selected Essays Exploring the Role of Cyber Operations in the Pursuit of National Interest*. National Defense University Press, Washington, D.C.

Chen, J. (2018). Does Conventional Deterrence Work in the Cyber Domain? *ECCWS 2018 17th European Conference on Cyber Warfare and Security V2*, Norway.

Crosignani, M., Macchiavelli, M. & Silva, A. (2021). *Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains*. Federal Reserve Bank of New York Staff Reports, no. 937.

Edwards, B., Furnas, A., Forrest, S. & Axelrod, R. (2017). Strategic aspects of cyberattack, attribution, and blame. *Proceedings of the National Academy of Sciences*, vol. 114, no. 11, pp. 2825–2830, 10.1073/pnas.1700442114.

Fischer, M. (2019). The Concept of Deterrence and Its Applicability in the Cyber Domain. *Connections QJ* 18, no. 1-2 (2019): 69-92. https://doi.org/10.11610/Connections.18.1-2.05.

Fischerkeller, M., Goldman, E., Harknett, R. (2022). *Cyber Persistence Theory: Redefining National Security in Cyberspace*. Oxford University Press, 2022. https://doi.org/10.1093/oso/9780197638255.001.0001.

Freedman, L. (2021). Introduction—The Evolution of Deterrence Strategy and Research. In: Osinga, F., Sweijs, T. (eds) *NL ARMS Netherlands Annual Review of Military Studies 2020*. NL ARMS. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-419-8_8.

Huskaj, G. (2019). The Current State of Research in Offensive Cyberspace Operations. *Proceedings of the 18th European Conference on Cyber Warfare and Security*, 2019, pp. 660–667.

Klimburg, A. (2020). Mixed Signals: A Flawed Approach to Cyber Deterrence. *Survival*, 62:1, 107-130, DOI: 10.1080/00396338.2020.1715071.

Kostyuk, N. (2021). Deterrence in the Cyber Realm: Public versus Private Cyber Capacity. *International Studies Quarterly*, Volume 65, Issue 4, December 2021, Pages 1151–1162, https://doi.org/10.1093/isq/sqab039 .

Kukkola, J. (2018). Civilian and military information infrastructure and the control of the Russian segment of Internet. *2018 International Conference on Military Communications and Information Systems (ICMCIS),* Warsaw, Poland, 2018, pp. 1-8, doi: 10.1109/ICMCIS.2018.8398700.

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, Doctoral Dissertation. Tampere: PunaMusta.

Lee, W.H., (2015). The Challenges of Cyber Deterrence. *Pointer, The Journal of the Singapore Armed Forces*. Vol.41 NO.1. ISSN 2017-3956.

Lindsay, J. (2015). Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity*, 1(1), 2015, 53–67. doi: 10.1093/cybsec/tyv003.

Lindsay, J. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22:365–404, 2013. doi: 10.1080/09636412.2013.816122.

Lonergan, E., & Lonergan, S. (2023). *Escalation Dynamics in Cyberspace*, Oxford University Press, Incorporated. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/ndul/detail.action?docID=7214000 .

Mareš, M. & Netolická, V. (2020). Georgia 2008: Conflict Dynamics in the Cyber Domain, *Strategic Analysis*, 44:3, 224-240, DOI: 10.1080/09700161.2020.1778278.

Mazarr, M. (2021). Understanding Deterrence. In: Osinga, F., Sweijs, T. (eds) *NL ARMS Netherlands Annual Review of Military Studies 2020*. NL ARMS. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-419-8_8.

Mellor, S. (2022). *Experts say Russia's war on Ukraine is accelerating the 'splinternet.' But what is the splinternet?* Fortune. https://fortune.com/2022/03/22/russia-war-ukraine-great-firewall-splinternet-internet/ .

Miadzvetskaya, Y. & Wessel, R. (2022). The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox. *7(1) European Papers 2022*, University of Groningen Faculty of Law Research Paper No. 27/2022. https://ssrn.com/abstract=4199627 .

Montgomery, E. (2020). Signals of strength: Capability demonstrations and perceptions of military power, *Journal of Strategic Studies*, 43:2, 309-330. doi: 10.1080/01402390.2019.1626724.

Muhammad, M., Basel K. & Vasileios G. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture, *Computers & Security*, Volume 88/ 2020. https://doi.org/10.1016/j.cose.2019.101636.

Navicky, M. & Tkach, B. (2023). Cross-Domain Cyber Incidents and State Responses. In Billingsley, J. (ed), *Integrated Deterrence and Cyberspace, Selected Essays Exploring the Role of Cyber Operations in the Pursuit of National Interest*. National Defense University Press, Washington, D.C.

Osula, AM. (2022). Building Cyber Resilience: The Defensive Shield for the EU. In: Boulet, G., Reiterer, M., Pardo, R.P. (eds) *Cybersecurity Policy in the EU and South Korea from Consultation to Action. New Security Challenges*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08384-6_9.

Portnoy, A. (2010). Pwn2Own wrap up and analysis. *Network Security*, Volume 2010, Issue 4,2010, Pages 4-5, https://doi.org/10.1016/S1353-4858(10)70043-X.

Puusa, A. & Juuti, P. (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät*. Helsinki: Gaudeamus.

Smeets, M. (2022). The Role of Military Cyber Exercises: A Case Study of Locked Shields, *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon),* Tallinn, Estonia, 2022, pp. 9-25, doi: 10.23919/CyCon55549.2022.9811018.

Soesanto, S. & Smeets, M. (2021). Cyber Deterrence: The Past, Present, and Future. In: Osinga, F., Sweijs, T. (eds) *NL ARMS Netherlands Annual Review of Military Studies 2020.* NL ARMS. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-419-8_20.

Soesanto, S. (2023). Ukraine's IT Army, *Survival*, 65:3, 93-106, doi: 10.1080/00396338.2023.2218701.

Sweijs, T. & Zilincik, S. (2021). The Essence of Cross-Domain Deterrence. In: Osinga, F., Sweijs, T. (eds) *NL ARMS Netherlands Annual Review of Military Studies 2020.* NL ARMS. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-419-8_8.

Taddeo, M. (2018). The Limits of Deterrence Theory in Cyberspace. *Philos. Technol*. 31, 339–355 (2018). https://doi.org/10.1007/s13347-017-0290-2.

Tor, U. (2017). 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence. In *Journal of Strategic Studies*, 40:1–2, (s. 92–117). https://doi.org/10.1080/01402390.2015.1115975.

Van der Meer, S. (2015). Enhancing International Cyber Security: A Key Role for Diplomacy. *Security and Human Rights.* 26. 193-205. https://doi.org/10.1163/18750230-02602004 .

Virtanen, T. & Simola, P. (2022). Layer 8 Tarpits: Overwhelming Malicious Actors with Distracting Information. In *Proceedings of the 21st European Conference on Cyber Warfare and Security.*

Wakefield, J. (2019). *Russia 'successfully tests' its unplugged internet*. BBC news. https://www.bbc.com/news/technology-50902496 .

Wanic, E. & Rowe, N. (2018). Assessing Deterrence Optinos for Cyber Weapons. *2018 International Conference on Computational Science and Computational Intelligence (CSC*I), Las Vegas, NV, USA, 2018, pp. 13-18, doi: 10.1109/CSCI46756.2018.00011.

Willett, M. (2022). The Cyber Dimension of the Russia–Ukraine War, *Survival*, 64:5, 7-26, DOI: 10.1080/00396338.2022.2126193.