The Concept of Comprehensive Security as a Tool for Cyber Deterrence

Maria Keinonen
National Defence University, Helsinki, Finland

maria.keinonen@mil.fi

Abstract: Cyber deterrence is often studied from the point of view of deterrence by punishment or offensive cyber strategies. A vast amount of studies claim that deterrence in cyberspace can never be successful with cyber means alone due to technical challenges and the problem of attribution. Some scholars argue that cyber resilience is an essential part of cyber deterrence, since not every cyberattack can be countered. These reviews are usually technical and concentrate on investigating the balance of offensive and defensive cyber strategies. The technical view leaves gaps in the physical and cyber-persona layers of cyberspace. This paper examines resilience from a societal perspective and reflects on the findings of cyber deterrence theories. The Concept of Comprehensive Security (CCS) is a Finnish model for building and sustaining resilience in society. Preparation for disruptive situations is carried out with the operating principle of overall safety, where society´s vital functions are protected in collaboration between the authorities, the business world, organisations, and citizens. The growing importance of cyber security has led to emphasising the importance of cyber resilience in the Concept of Comprehensive Security. This study investigates the possibilities to utilize the CCS as a tool for cyber deterrence and aims to create a new perspective on the international academic discussion of cyber deterrence. The research method is content analysis. The investigated material consists of Finnish CCS documents, as well as academic cyber deterrence and cyber resilience literature. The characteristics of the CCS are compared to the factors found in the cyber deterrence material to answer the research question. The key observation presented in this study is that a comprehensive approach to building resilience in the society is essential for the credibility of cyber deterrence. Resilience in cyberspace should be viewed from the perspective of every layer, including logical, physical and cyber-persona layers.

Keywords: Cyber deterrence, Finland, Concept of Comprehensive Security, resilience

1. Introduction

Numerous cyber threats target critical infrastructure of our digitalised society. The impact of the threat is widened by the fact that these critical systems have interdependencies, so disruptions in one system can affect several others. (Lehto & Neittaanmäki, 2022) By developing society's resilience, the ability to anticipate, withstand and recover from disruptions to critical infrastructure is improved.

Finland has a Concept of Comprehensive Security (CCS) for building and sustaining resilience in Finnish society. Preparation for disruptive situations is carried out with the operating principle of overall safety, where society´s vital functions are protected by the authorities, the business world, organisations, and citizens. The growing importance of cyber security has led to emphasising the importance of cyber resilience in the CCS. (The Security Committee, 2017)

This study investigates the possibilities to utilise the CCS as a tool for creating deterrence in cyberspace and aims to create a new perspective on the international academic discussion of cyber deterrence. The type of resilience the CCS creates and its possibilities to be utilised in cyber deterrence are investigated. The CSS, as a model from the perspective of cyberspace, is also examined. This study leaves out of scope the practical application of the concept and the assessment of its functionality.

The research question is: *"How can the Concept of Comprehensive Security be utilised in building cyber deterrence?"* This question is answered by analysing the CSS material and theories of resilience and cyber deterrence.

Resilience as part of deterrence is a controversial topic. There are views according to which resilience and defence widen the scope beyond deterrence (Borghard and Lonergan, 2021). On the other hand, it can be thought that resilience can be used to build a basis for deterrence, because it signals to the potential aggressor that attacks won´t have the desired effect (Sweijs and Zilizny, 2020; Reire, 2016).

This study examines resilience as a part of deterrence from the perspective of cyberspace. Cyberspace is dealt with through a threefold division, where it is divided into physical, logical and personal layers (Laari et al., 2019). All of these layers must be considered when planning resilience and deterrence. Therefore, the protection of cyberspace cannot consist solely of technical means applied to the logical layer.

2. Concept for Comprehensive Security and its connection to cyberspace

The Finnish model, the Concept for Comprehensive Security (CCS), involves all society's actors to prepare for disruptive situations. The concept's role is more coordinating than managing, it creates conditions for cooperation for the authorities, businesses as well as citizens and non-government organisations. The concept is implemented in practice in branch-specific or cross-administrative strategies and executive programmes. (The Security Committee, 2017) The Finnish national cyber security strategy is closely linked to the CCS, and it relies on the general incident management model. (Turvallisuuskomitea, 2019)

Comprehensive security can be understood as *"a condition where threats and risks to the vital functions of society are prepared for"* (Sanastokeskus, 2017). This includes *"preparing for threats, managing disturbances and exceptional conditions and recovering from them"* (Sanastokeskus, 2017).

A vital function can be described as *"a function that is necessary for the functioning of society"* (Sanastokeskus, 2017). Critical infrastructure can be understood as *"basic structures, services and related functions that are necessary to maintain the vital functions of society"* (Sanastokeskus, 2017). The critical infrastructure consists of both physical structures and electronic functions and services. For example, energy production, transmission and distribution systems, transport and logistics, information and communication systems and water and waste management are all part of critical infrastructure. (Valtioneuvosto, 2022)

The CCS identifies seven vital functions in society that are to be protected: 1) leadership and management, 2) international and European Union cooperation, 3) defence capability, 4) internal security, 5) economy, infrastructure and security of supply, 6) functional capacity of the population and services and 7) mental crisis resistance. (The Security Committee, 2017)

Public administration services enable the leadership and the management of the state as well as the international and European Union cooperation. This includes the decision-making ability and shared situational awareness. These services include the state's common information and communication services, the security network and support services. ICT (Information and Communication Technology) functions and the production of digital services are national and international, enabling international cooperation. (The Security Committee, 2017)

Defence capability includes military defence, society's preparedness and national authority cooperation and international defence cooperation. The ability to receive and give military aid is part of Finland's defence capability. (The Security Committee, 2017) Military capabilities are dependent on information processing, the ability to form situational awareness and control of weapon systems and logistic systems. (Valtioneuvosto, 2021)

By maintaining the internal security, crimes against the population are prevented and combated, also consequences of accidents and environmental damage or other similar disturbances and threats are managed. Internal security includes border security, maintenance of public order and security, rescue operations and protection of the population in accidents and dangerous situations. (The Security Committee, 2017) Authority networks and communication and situational picture services, including emergency response systems, are critical in maintaining internal security. (Sisäministeriö, 2019)

The economy, infrastructure and security of supply consist of services and networks, such as financial transactions, information and communication systems, digital services and information, logistics services and electricity systems. These vital functions have many interdependencies in cyberspace. For example, financial market services are completely dependent on the functionality of telecommunication connections, ICT systems and the related electricity supply. (The Security Committee, 2017)

The functional capacity of the population and services includes systems of social work and health services, education and research systems. For example, in terms of social and health care, it is essential to secure diagnostic capability and the storage and transfer of patient and customer data. (The Security Committee, 2017)

Mental crisis resistance is the ability of an individual, community and society to withstand the mental pressure caused by crises and cope with their effects. Maintaining citizens' trust is essentially dependent on the communication of authorities, organisations and other communities in exceptional circumstances. The media plays a significant role in the nation's mental crisis resistance as the maintainer and creator of crisis resilience. (The Security Committee, 2017)

Table 1 summarises the vital functions and their connection to cyberspace mentioned in the CCS. It should be noted that these functions are not separate from each other, but they form an interconnected system where a malfunction in one could cause disturbances in one or several other functions (Valtioneuvosto, 2022).

Table 1: Vital functions in Finnish society and their connection to cyberspace.

Vital functions	Examples of connection to cyberspace
Leadership and management	Situational awareness, crisis communication, information sharing
International and European Union cooperation	Information systems and the Internet
Defence capability	Systems, networks and connections of the defence forces and authorities
Internal security	Authorities' systems, networks and connections, crisis and emergency communication, logistics, social and healthcare systems
Economy, infrastructure and security of supply	Financial transactions, information and communication systems, digital services and information, logistics, electricity
Functional capacity of the population and services	Systems of social work and health services, education and research systems
Mental crisis resistance	Crisis communication services, media

According to the Cyber Security Strategy 2013 (CSS13), Finland's vision of cyber security is the following: *"Finland can protect its vital functions in all situations against the cyber threat*" (Turvallisuuskomitea, 2013). These functions mentioned in the CSS13 are similar to the functions presented in table 1. The CSS13 states that national cyber resilience is measured in such a way that it can create preparedness by the goals of overall safety, the ability to function in cyber-disruption situations and recovery after cyber-disruptions and resilience. The goal is achieved by maintaining and developing the ability of companies and organisations to detect and combat cyber threats and disruptions, as well as to recover from them. Necessary protective capacity is maintained and resilience is developed for example by planning and using backup methods. (Turvallisuuskomitea, 2013)

3. Methods and results

This study investigates the resilience created by the CCS and how this resilience can be utilised in cyber deterrence. Content analysis (Puusa, 2021) was used as a research method. The material concerning resilience and cyber deterrence was gathered from the abstract and citation database Scopus. The search phrases included the terms *"cyber deterrence"* and *"resilience in cyberspace".* Purely technical articles were excluded, because they were out of the strategic perspective of this study. The search generated seventeen articles on cyber deterrence and nine articles on resilience in cyberspace. The material concerning the CCS was searched from the websites of the Finnish Government. This material consists of seven Finnish strategic documents. Analysed articles and documents are cited in the text.

Two hypotheses for the study were set based on previous cyber deterrence studies. Because deterrence implemented exclusively in cyberspace through cyber means has proven to be a difficult concept (Wei, 2015; Brantly, 2018), this study sets the first hypothesis as follows: *"deterrence in cyberspace is created by a wide selection of means".* In addition to cyber-specific means, these include political, economic, military and legal means, as well as resilience, which are used for defensive or offensive purposes (Brantly, 2018; Bendiek and Metzger, 2015; Burton, 2018; Chen, 2017).

The second hypothesis is that *"resilience is essential for cyber deterrence".* This was based on two assumptions: 1) not all cyberattacks can be prevented (Lindsay, 2015; Klimburg, 2012; Nye, 2017) and 2) the ability to recover can be used to demonstrate that the attack does not achieve the desired effects (Nye, 2017; Vogel et al., 2021; Kerttunen, 2019).

The first round of analysis consisted of the collected cyber deterrence material. The aim was to form an understanding of functional ways to create deterrence in cyberspace, supporting the first hypothesis. This view was deepened by studying the role of resilience in cyberspace in the second analysis round. The findings from the first two analysis rounds were compared to the third analysis round, where the CSS material was investigated from the perspective of cyberspace and its three layers. Gathering and comparing the results of these rounds formed the answer to the research question: *"How can the Concept of Comprehensive Security be utilised in building cyber deterrence?"*

3.1 Cyber deterrence

According to the hypotheses, cyber deterrence is best created with a wide selection of means that should not be limited just to cyberspace, although technical and cyberspace-targeted means should not be forgotten. These

means could include, for example, developing a regulatory framework against cyber-attacks and disruptions (Chen, 2017), developing resilience to recover from cyber-attacks (Vogel et al., 2021; Kerttunen, 2019; Burton, 2018; Tolga, 2018; Nye, 2017), creating international rules on acceptable activity and the legitimacy of targets in cyberspace (Chen, 2017; Bendiek and Metzger, 2015; Russell, 2015) and a national strategy for creating cyber deterrence (Bendiek and Metzger, 2015).

Resilience and functional security practices are likely to increase the cost of aggressions, therefore creating additional denial thresholds (Vogel et al., 2021; Kerttunen, 2019; Nye, 2017). This can be achieved, for example, through active cyber defence (Hurley and Watkins, 2016; Bendiek and Metzger, 2015). This requires real-time monitoring and threat detection capabilities, analysis capabilities and the ability to reduce the impact of threats. (Jasper, 2015)

Active cyber defence creates opportunities to deny the impact of the opponent's actions through resilience and to cause losses to the opponent by employing countermeasures. (Borghard and Lonergan, 2021; Jasper, 2015) Countermeasures should consider the possibility of kinetic retaliation if a cyberattack seriously damages the physical infrastructure or threatens the lives of citizens. (Chen, 2017; Bendiek and Metzger, 2015) Other means for retaliation are, for example, legal actions, financial sanctions or diplomatic isolation. (Burton, 2018)

Cyber deterrence needs to be created through the cooperation of different actors. These include both national and international organisations and authorities, as well as public and private sector actors. The deterrence created in this way is directed against state actors, threats within the state, as well as crime and terrorism. (Burton, 2018)

Both society and policymakers need to accept that there are areas where cyberattacks can´t be deterred. It should be noted that cyber deterrence needs prioritising, since cyber defence cannot be strong everywhere. (Kerttunen, 2019; Tolga, 2018; Lindsay, 2015; Klimburg, 2012) At a minimum, such cyber-attacks should be countered that have strategic effects by damaging national security and vital functions (Kostyuk, 2019). Cyber deterrence should not be treated as a separate strategy, but as a part of the state´s comprehensive deterrence and other strategies aiming to protect cyberspace. (Brantly, 2018; Lonsdale, 2018) For this, it is worth using existing structures and operating models. (Tolga, 2018)

In this article, cyber deterrence refers to the actions taken to convince an aggressor that an attack in cyberspace is not profitable, and it may cause counter-measures. The selection of means includes political, economic, military and legal means, as well as resilience. Therefore, cyber deterrence is created by the whole society, including authorities, as well as organisations and citizens. Cyber deterrence is understood to be part of the state´s comprehensive deterrence.

3.2 Resilience in cyberspace

Resilience can be understood as an internal characteristic of the object and as an interactive recovery process activated in times of crisis. (Hyvönen et al., 2019) Activities, such as anticipating, resisting, recovering, detecting and adapting to threats of any kind, are associated with resilience. (Vogel et al., 2021)

Resilience can be described as the ability of individuals and communities to *"maintain the ability to function in changing conditions and the readiness to face disruptions and crises and recover from them"* (Sanastokeskus, 2017). Resilience is used to respond to situations where safety is compromised by unexpected activity. (Sanastokeskus, 2017)

From a broader perspective, resilience can also be found in the attitudes and images of individuals, it can be seen in public debate and the shared values and goals of society. Resilience can be thought of as part of social capital. Making it public creates the citizen's trust in society and manifests itself, for example, in national narratives. (Rodin, 2015)

The resilience of information systems can be understood as *"the ability of an information system to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities, and to recover to an effective operational posture in a time frame consistent with mission needs*" (NIST, 2020). This includes two kinds of continuous capabilities, the first being the ability to continue services under disruption and the second the ability to restore the effective operating state within a tolerable time frame. (Zuo et al., 2021)

Most of modern society's functions are dependent on cyberspace. Cyber disruption situations can cause harm to several critical services and functions. Therefore, cyber resilience should be considered as a whole, which

includes physical, informational, cognitive and social dimensions. (Bellini and Marrone, 2020) Cyber resilience can be described as *"the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems and it can still maintain a certain functional service capability*" (Zuo et al., 2021).

Cyber resilience can be approached as a combination of cyber security and society's crisis resilience. The continuity of society's critical services is ensured by the cooperation of several actors. These are governmental actors and those operating from critical infrastructure and online services. (Devanni et al., 2022; Burton, 2018)

Based on the definitions presented, resilience in cyberspace consists of actions that aim to preserve the system's vital functions or services in the event of a disruption and to restore or replace them within a desired timeframe. Resilience includes the ability to anticipate and detect disruptions and to learn from previous disruptions. It should also be noted that cyber resilience is not only technical or physical, because disruptions in cyberspace affect services used by people. The human dimension of cyber resilience includes mental resilience. In today's world, where information and services are immediately available, disruptions may cause mental pressure on the individual.

3.3 The Concept of Comprehensive Security and cyberspace

Understanding cyberspace is facilitated by dividing it into layers, each of which has a different role in processing information. This study adopts the Finnish view, which originates from the U.S. publication *JP 3-12, Cyberspace Operations* (US Joint Chiefs of Staff, 2018). This view divides cyberspace into three layers: physical, logical and cyber-persona.

The physical layer contains the geographical and physical network components used to store, transfer and process information. It includes hardware, systems and infrastructure that make up physical routes and networks. (Laari et al., 2019) From the critical infrastructure point of view, the physical layer includes the facilities where the equipment used by vital services, and the personnel who operate them, are geographically located. This also includes the physical devices involved in data transfer and data storage, for example, servers and sea cables. (The Security Committee, 2017)

The CSS builds resilience into physical cyber-infrastructure in various ways. Usability and safety of the necessary facilities and equipment are ensured in all situations. The supply of electricity is secured for critical services. Procurement chains are secured by national self-sufficiency, production and international agreements. Physical data transmission connections are secured and provisions are made for switching to backup systems. (Valtioneuvosto, 2022) The domestic cyber security industry is being developed to secure services. (Paananen, 2021)

The logical layer comprises logically programmable parts of the network. Logical components are not tied to a specific physical location. The layer consists of network settings, information security processes, data transfer protocols, internet domain names, ownership information and information, applications and protocols that control interaction with the physical layer. (Laari et al., 2019) From the point of view of critical infrastructure, the logical layer includes all the networks, systems and digital services which are needed for the vital functions of society. (Valtioneuvosto, 2022)

As a part of cyber resilience, the built-in security of national network services is being developed. The operation and safety of information reserves, services and systems critical to society are ensured throughout their entire life cycle. (Paananen, 2021) The interdependencies of the digital operating environment require an overall architecture that takes cyber security into account. (Security Committee, 2019)

The goal of cyber security is to identify and detect possible disruptions to vital functions and minimise the harmful effects of disruptions. (Security Committee, 2019) This also requires comprehensive cyber security situational awareness. (Paananen, 2021) Key players are building their resilience, including planning and practicing backup methods to operate under and recover from cyberattacks. Legislation must support the protection of society's vital functions and state security against cyber threats. (Turvallisuuskomitea, 2013)

The cyber-persona layer contains the virtual identities of individuals or communities in cyberspace. An individual or community can have simultaneously several cyber personalities. On the other hand, several people can share one cyber persona, for example, using a single e-mail account for many users. (Laari et al., 2019) From the perspective of critical infrastructure, the cyber-persona layer consists of virtual identities of personnel and organisations connected to the vital functions of society. Using these identities requires the person to have

sufficient information security knowledge and to be aware of possible threats targeted to usernames and passwords, for example, various means of social engineering. Also, people themselves are a critical part of the cyber-persona layer. (Laari et al., 2019)

The CSS builds resilience into the cyber-persona layer by developing the competence of individuals and organisations. (Turvallisuuskomitea, 2019) The goal is that every citizen, from a child to a pensioner, has sufficient skills to function in a digital society. Also, secure services must be nationally produced. Cybersecurity skills are needed both by the producers of the services and by the citizens using them. (Paananen, 2021)

Mental resilience is needed for the resilience of the cyber-persona layer, since severe cyberattacks could cause mental pressure on individuals. At the core of mental crisis resilience is the sharing of information through reliable communication and training. Organisations produce information for authorities and decision-makers about citizens' security needs, so communication works in both directions in an ideal situation. (The Security Committee, 2017)

The resilience to cyberspace produced by CCS is a complex entity that consists of the measures of many actors in society, security of supply, technology, backup systems and people's competence. Table 2 describes the results of the analysis described above.

Table 2: The CCS from the perspective of cyberspace.

Cyberspace layer	Critical infrastructure and vital functions connected to cyberspace	Resilience produced by the CSS
Logical	Networks, systems and digital services, which are needed for the vital functions of society.	Ability to detect, identify, analyse and minimise threats, situational awareness, backup methods, built-in security.
Physical	Facilities where the equipment used by vital services and the personnel who operate them are located. This also includes the physical devices involved in data transfer and data storage.	Usability and safety of facilities and equipment, secured electricity supply, national self-sufficiency, production and international agreements on material supply, secured data connections, backup systems, domestic industry.
Cyber-persona	People, cyber-identities of individuals and organisations.	Competence, mental resilience.

Figure 1 shows the impact of cyber resilience on cyber deterrence from the perspective of the three layers of cyberspace. Cyberspace is an integral part of society's critical infrastructure and functions, as they are connected to it in several ways. Resilience must be built into every layer of cyberspace, because a disruption in one layer affects the others.

The CCS considers the physical, digital and human aspects of society's critical infrastructure. Therefore, it creates resilience also for cyberspace that can be utilised for cyber deterrence. It should be noted, however, that from the cyber deterrence point of view, it is necessary to identify the aspects that can be used from the already existing cyber resilience, but also the gaps that the existing models do not respond to.

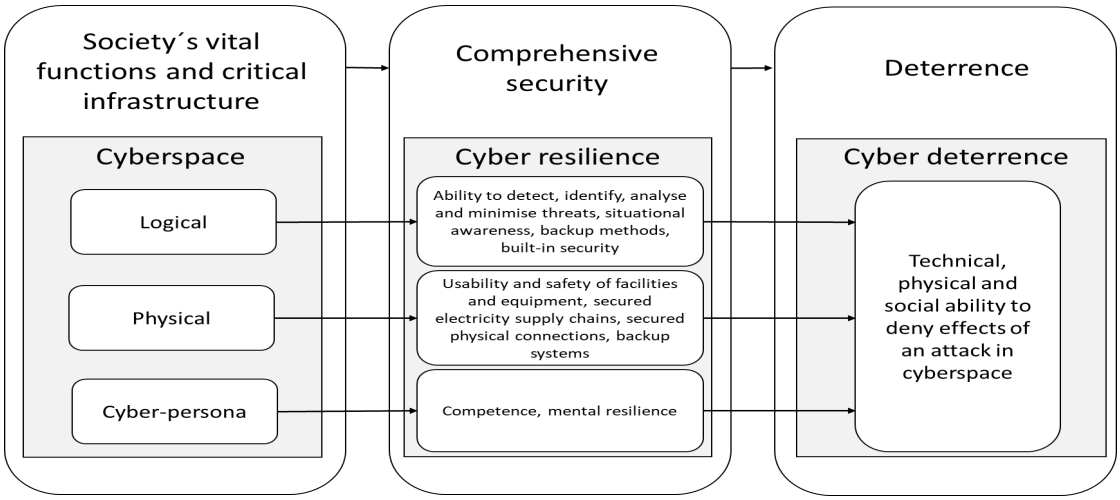

Figure 1: The CCS as a tool for cyber deterrence.

4. Conclusion

Looking at cyberspace as a whole, which includes a physical, logical and personal layer, resilience must be built into each of these. Most cyber deterrence studies focus on the logical layer and technical solutions, but the other two layers should not be forgotten. The resilience of the cyber-persona layer consists of the individuals and their cyber security expertise. The security of the physical layer is connected to the sovereignty of the state in the traditional sense.

Cyberspace affects society´s critical functions directly, because they connect to it in one way or another. By developing technical, physical and mental resilience, cyber disruptions are better tolerated. In Finland, CCS is an existing structure that can be publicly signalled to convince the aggressor of society's ability to withstand hostile actions. This creates deterrence, because the execution of the attack as planned or the planned impact is disputed.

Cyber deterrence is best created using all means available, including political, economic, legal and military capabilities. Because the adversary can always question the defender´s will to retaliate or attack, signalling resilience is a more plausible way to convince the opponent that the attack will not achieve the desired effects. However, for the sake of credibility and to be proactive, the state must also have the ability and publicly signalled will to retaliate.

It should be noted, that shortcomings have occurred in the practical application of the CCS, for example, during the COVID-19 pandemic (Tulevaisuusvaliokunta, 2020). Therefore, the results of this study must be viewed critically from the point of view that the functionality of the concept was not evaluated in practice. The subject of further research is whether the tasks and instructions given by the strategic documents can really be implemented according to the CCS.

The results of this study could be deepened in further research by investigating how narratives existing in society could be utilised in deterrence signalling, such as the importance of the resilience produced by CSS to society's crisis resistance. It is advantageous for the state to use functions of society already in place in deterrence signalling, even if they produce deterrence as a by-product.

References

Bellini, Emanuele and Stefano Marrone (2020). Towards a novel conceptualization of Cyber Resilience, *2020 IEEE World Congress on Services (SERVICES),* Beijing, China. DOI: 10.1109/SERVICES48979.2020.00048.

Bendiek, A., & Metzger, T. (2015). *Deterrence theory in the cyber-century*. Lessons from a state-of the-art literature review. https://doi.org/10.1007/s13347-017-0290-2

Borghard, Erica & Shawn Lonergan (2021). Deterrence by denial in cyberspace, *Journal of Strategic Studies*. DOI: 10.1080/01402390.2021.1944856.

Brantly, Aaron (2018). The Cyber Deterrence Problem. T. Minárik, R. Jakschis, L. Lindström (Eds.). *2018 10th International Conference on Cyber Conflict*. DOI:10.23919/CYCON.2018.8405009.

Burton, J., (2018). *Cyber Deterrence: A Comprehensive Approach?* Nato Cooperative Cyber Defence Centre of Excellence, Estonia 2018. https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf

Chen, Jim (2017). Deterrence and its implementation in cyber warfare. In *International Conference on Cyber Warfare and Security*. Academic Conferences International Limited. https://www.jstor.org/stable/26633152

Devanny, Joe, Luiz Goldoni and Breno Medeiros (2022). Strategy in an Uncertain Domain: Threat and Response in Cyberspace. *Journal of Strategic Security 15*, no. 2. https://doi.org/10.5038/1944-0472.15.2.1954

Hurley, John and Lanier Watkins (2016). Cyberspace: The new Battlefield. In *11th International Conference on Cyber Warfare and Security*. Academic Conferences International Limited.

Hyvönen, Ari-Elmeri; Tapio Juntunen, Harri Mikkola, Juha Käpylä, Harri Gustafsberg, Markku Nyman, Tiina Rättilä, Sirpa Virta, Johanna Liljeroos (2019). *Kokonaisresilienssi ja turvallisuus: tasot, prosessit ja arviointi.* Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 17/2019. https://www.fiia.fi/wp-content/uploads/2019/02/17-2019-kokonaisresilienssi-ja-turvallisuus.pdf

Jasper, S. (2015). Deterring Malicious Behavior in Cyberspace. *Strategic Studies Quarterly*, 9(1), 60–85. https://www.jstor.org/stable/26270834

Kerttunen, Mika (2019). Beyond Punishment: Deterrence in the Digital Realm. *Connections*, 18(1/2), 61–68. https://www.jstor.org/stable/26948849

Klimburg, Alexander (Ed.) (2012). *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

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

Laari, T., Flyktman, J., Härmä, K., Timonen, J. & Tuovinen, J. (2019). *#kyberpuolustus: Kyberkäsikirja Puolustusvoimien henkilöstölle*. National Defence University, Finland. https://urn.fi/URN:ISBN:978-951-25-3120-2

Lehto, Martti & Pekka Neittaanmäki (2022). *Cyber Security: Critical Infrastructure Protection.* Cham, Switzerland: Springer (Computational Methods in Applied Sciences). https://doi.org/10.1007/978-3-030-91293-2

Lindsay, Jon (2015). Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack, *Journal of Cybersecurity*, Volume 1, Issue 1, September 2015. https://doi.org/10.1093/cybsec/tyv003

Lonsdale, David (2018). Warfighting for Cyber Deterrence: A Strategic and Moral Imperative. *Philosophy & Technology*. 31. DOI: 10.1007/s13347-017-0252-8

National Institute of Standards and Technology NIST (2020). *Security and Privacy Controls for Information Systems and Organizations.* Special Publication 800-53, Revision 5. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Nye, J. (2017). Deterrence and Dissuasion in Cyberspace. *International Security 2017*; 41 (3): 44–71. DOI:10.1162/ISEC_a_00266

Paananen, Lauri (2021). *Kyberturvallisuuden kehittämisohjelma.* Liikenne- ja viestintäministeriö, Helsinki Finland. ISSN 1795-4045 pdf. http://urn.fi/URN:ISBN:978-952-243-599-6

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

Reire, Gunda (2016). Resilience Challenges in the Baltic Countries. In Andžāns M, Bruģe I (eds) *The Baltic Sea Region: Hard and Soft Security Reconsidered*. Latvian Institute of International Affairs, Riga.

Russell, Alison (2015). Strategic Anti-Access/Area Denial in Cyberspace. *2015 7th International Conference on Cyber Conflict.* NATO CCD COE Publications, Tallinn. https://ccdcoe.org/uploads/2018/10/Art-11-Strategic-Anti-Access-Area-Denial-in-Cyberspace.pdf

Rodin Judith (2015). *The Resilience Dividend; Managing Disruption, Avoiding Disaster, and Growing Stronger in an Unpredictable World*. Profile Books, London.

Sanastokeskus (2017). *Vocabulary of Comprehensive Security*. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

Sisäministeriö (2019). *Kansallinen riskiarvio 2018*. Sisäministeriön julkaisuja 2019:5. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161332/5_2019_Kansallinen%20riskiarvio.pdf

The Security Committee (2017). *The Security Strategy for Society*, Government Resolution / 2.11.2017, Finland. https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

Tolga, Ihsan Burak (2018). *Principles of Cyber Deterrence and the Challenges in Developing a Credible Cyber Deterrence Posture*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn. https://ccdcoe.org/uploads/2018/10/Challenges_in_Developing_Credible_Cyber_Deterrence_Posture_in_Cyberspace-1.pdf

Turvallisuuskomitea (2013). *Suomen kyberturvallisuusstrategia.* Finland. https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf

Turvallisuuskomitea (2019). *Suomen kyberturvallisuusstrategia 2019.* Finland. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

Tulevaisuusvaliokunta (2020). *Koronapandemian hyvät ja huonot seuraukset pitkällä aikavälillä.* Eduskunnan tulevaisuusvaliokunnan julkaisu 1/2020. https://www.eduskunta.fi/FI/naineduskuntatoimii/julkaisut/Documents/tuvj_1+2020.pdf

Sweijs, Tim & Samuel Zilincik (2020). The Essence of Cross-Domain Deterrence. In Osinga, Frans & Tim Sweijis (eds). *Deterrence in the 21st Century—Insights from Theory and Practice*. Netherlands Annual Review of Military Studies 2020. https://doi.org/10.1007/978-94-6265-419-8_8

US Joint Chiefs of Staff (2018). *JP3-12 Cyberspace Operations*. https://irp.fas.org/doddir/dod/jp3_12.pdf

Valtioneuvosto (2022). *Valtioneuvoston huoltovarmuusselonteko*. Työ- ja elinkeinoministeriö. http://urn.fi/URN:ISBN:978-952-383-803-1

Valtioneuvosto (2021). *Valtioneuvoston puolustusselonteko*. Valtioneuvoston julkaisuja 2021:78. http://urn.fi/URN:ISBN:978-952-383-820-8

Vogel, Elisabeth, Zoya Dyka, Dan Klann, and Peter Langendörfer (2021). "Resilience in the Cyberworld: Definitions, Features and Models" Future Internet 13, no. 11: 293. DOI:10.3390/fi13110293

Wei, Lee Hsiang (2015). The Challenges of Cyber Deterrence. *Pointer, The Journal of the Singapore Armed Forces*. Vol.41 NO.1. ISSN 2017-3956. https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/POINTER_Vol41_1.pdf

Zuo, Jinxin, Ziyo Guo, Jiefu Gan and Yueming Lu (2021). Enhancing Continuous Service of Information Systems Based on Cyber Resilience, *2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC)*, Shenzhen, China. DOI: 10.1109/DSC53577.2021.00085.