Using Military Cyber Operations as a Deterrent

Maria Keinonen
National Defence University, Helsinki, Finland

maria.keinonen@mil.fi

Abstract: The Deterrence theory was formed after the World War II to describe the tensions between nuclear-armed states. Because of its origins, deterrence is mainly researched from the point of view of powerful states. However, deterrence nowadays is essential for any state to include in their strategies. The ever-increasing dependence on technology forces states to protect their sovereignty in cyberspace as well as in other domains. Therefore, cyber operations should be considered not just as a means to protect the cyber domain, but as means of deterrence. Cross domain deterrence (CDD) is a theory that includes all the warfighting domains in creating deterrence, including cyberspace. Despite these new perspectives, the use of military cyber operations as a deterrent has been studied mainly in terms of offensive strategies. Therefore, incorporating all types of military cyber operations into deterrence strategies is understudied. This study focuses on the possibilities of a small state to use cyber operations to create deterrence. The research question is: "How can a small state use cyber operations as a deterrent?" According to the Finnish understanding, cyber operations can be divided into three types: offensive, defensive and supportive operations. These types of operations each have their separate role in securing the cyber domain and freedom of action in every military domain, as well as influencing the opponent´s ability to act as planned. Using Finland as a case study, this paper argues that using military cyber operations is noteworthy for any state dependent on cyberspace, not only for military purposes, but for building CDD. The CDD theory and characteristics of cyber operations are studied in order to form better understanding of the topic and provide ideas for academic discussion. The research methods are content and SWOT analysis. The key observation presented is that each type of cyber operation has a role in forming CDD. For a small state, it´s profitable to use every type of cyber operations and thus expand the tool box for deterrence.

Keywords: Cross Domain Deterrence, Cyber Deterrence, Finland, Offensive Cyber Operation, Defensive Cyber Operation, C5 operation, Cyber Resilience

1. Introduction

The core idea of deterrence can be summed up as an effort to convince the other party that a hostile action is not profitable and both can achieve their goals without provoking the other into conflict (Mazarr & Goodby, 2010). For a small state this is a continuous battle of being credible enough, but not too provocative in the eyes of a bigger adversary. It can be questioned, if a small state has the ability to build deterrence with a credible threat (Hanska, 2019) or if deterrence is in general more of a bargaining process with something valuable for both parties to gain or lose (Kerttunen, 2019).

The Deterrence theory was formed after the World War II to describe the tensions between nuclear-armed states. It focused purely on the use of military force, especially nuclear weapons, and its prevention (Morgan, 2003). With the development of technology and the threat environment becoming more diversified with threat actors, the classic way of structuring deterrence was no longer sufficient. (Arie, 2016). The toolbox of deterrence must be expanded including political, economic, diplomatic and military means. (Sweijs, T., Zilincik, 2021)

Because of its origins, deterrence is mainly researched from the point of view of powerful states. However, deterrence nowadays is essential for any state to include in their strategies. The ever-increasing dependence on technology forces states to protect their sovereignty in cyberspace as well as in other domains. This paper focuses on the possibilities of a small state to use cyber operations to create deterrence. The research question is: "How can a small state use cyber operations as a deterrent?"

The concept of a small state can be addressed via materialistic values, as relatively smaller territories, populations and resources than surrounding neighbours (Radoman, 2018). It can also be considered as a deficit in influence and autonomy in position of international relationships (Goetsel, 2000). Small states are relatively more vulnerable for international security threats with limited options to mitigate them compared to their bigger counterparties (Väyrynen, 1997). Small states are expected to favour international cooperation that strengthens common norms and institutions in international security (Coolsaet, 2004).

A small state in this paper refers to a state with relatively lower population and fewer resources than its neighbouring countries and with an intention to strengthen international norms to stabilize the global threat environment. A small state must use every cost-effective means of creating deterrence, even if the end result is uncertain (Toomse, 2015). This research understands cost as a combination of time, money, human recourses and technology spent to achieve a goal.

Finland has been chosen as the subject of the article's case analysis, because it meets the aforementioned criteria of a small country. Finland shares more than a thousand kilometres of border with Russia, and for more than a hundred years it has managed its relations with its more powerful neighbour, without a military alliance. This changed in the spring of 2022 after Finland applied to become a member of NATO, but the country's security policy solutions have nevertheless been shaped during a time when Finland has remained militarily non-aligned throughout its independence.

2. Background

2.1 Cross domain deterrence

Cross domain deterrence (CDD) can be understood as the use of a threat or a combination of them to dissuade a target from taking actions of any type (Lindsay & Gartzke, 2019). CDD can be viewed as the use of military force in all domains of warfare. An attack in one domain can be answered by action in another domain, so warfare does not have to be completely symmetrical. A broader approach includes non-military elements to the CDD theory, such as political means and economic sanctions. (Sweijs & Zilincik, 2021)

This paper refers to military domains (air, land, sea, space, cyber) as “domains” and. Military domains together with non-military elements (diplomatic, information, economic, legal) are referred as “dimensions” according to a DIMEL (Diplomatic, Information, Military, Economic, Legal) model (Sweijs et al, 2021). Military operations, including cyber operations, are considered to be set of actions in military domains to achieve a mission or goal set for a military force (JP 3-0, 2017). Cyberspace is referred to the cyber environment of the whole society including the military cyber domain.

A comprehensive approach might create in smaller states an opportunity to exercise deterrence without risking too much in provoking bigger adversary, especially while acting with other states with similar goals (Toomse, 2015). An example of this is Finland participating in European Union economic sanctions against Russia because of the war in Ukraine.

The CDD theory broadens the use of available capabilities to make symmetric or asymmetric moves. It increases the synergy between these capabilities and creates a portfolio for deterrence options. It also commits society's actors more broadly to building deterrence. (Lindsay & Gartzke, 2019) The ability to create asymmetry might act as a benefit for a small state, since it´s not always profitable to face a greater power with similar means. Also, involving actors in the whole society adds resources to building deterrence.

It could be asked if CDD diminishes the importance of deterrence by broadening the view beyond the use of nuclear and military power and is thus doomed to failure, because the softer means are less likely to deter threats. (Gartzke & Lindsay, 2017a) On the other hand, deterrence is no longer see as an absolute concept as it was in the last century. Rather, it is a competition where states take turns climbing the escalation steps with their opponents. (Lindsay & Gartzke, 2017b)

CDD's idea that a threat in one domain can also be countered in another domain is also well suited to deter threats in cyberspace. Combating cyber threats with cyber means alone can never be complete, since building cyber defence is slow and expensive compared to executing cyberattacks. Inevitably, there will always be attack vectors to be exploited in the cyberspace. (Taddeo, 2018a) Instead of countering every cyberattack possible, it is more efficient to draw the line between what is absolutely reprehensible and will cause countermeasures (Rivera, 2015). This could increase the credibility of deterrence.

2.2 The role of military cyber operations in Finland

Finland divides cyber operations into three types: offensive cyber operations (OCO), defensive cyber operations (DCO) and Command, Control, Communications, Computers, Collaboration operations (C5O). Cyber operations also involve control of the battle space, intelligence and modification of the battle space, just like any other military operation, but instead of the physical domains, the actions are aimed at the cyber domain. These are actions supporting cyber operations. (Laari et al, 2019)

Defensive cyber operations protect friendly cyber domain and they are carried out against a specific threat. The goal is to prevent or disrupt the adversary's actions and restore the safety of compromised cyberspace. Protective measures (Defensive Cyber Operation Internal Defence Measures, DCO-IDM) consist of active and proactive means to detect and respond to a threat factor within the friendly cyberspace. The countermeasures

(Defensive Cyber Operation Responsive Actions, DCO-RA) extend beyond the cyberspace to be protected. It requires that the origin of the attack has been verified. (Laari et al, 2019)

The goal of offensive cyber operations is to project power in or through a foreign cyberspace to support one's own goals. OCO can target targets in the adversary's cyberspace or cause effects in the physical domain. (Laari et al, 2019)

C5 operations secure and maintain elements of friendly cyber domain. Unlike defensive cyber operations, C5O are not carried out against any specific threat, but are used to prepare against all threats that weaken friendly cyber domain. C5O can be understood as a continuous operation for cyber security maintenance. (Laari et al, 2019)

In Finland, the statutory duties of the Finnish Defence Forces (FDF) require the defence of national security in the event of a military attack (11.5.2007/551, 2007), and this also applies to the defence of state sovereignty in the cyberspace against state actors (Finnish Government, 2021). Military cyber defence capability consists of intelligence, offensive and defensive capabilities (Puolustusministeriö, 2019).

According to the Governments Defence Report 2021, not only the FDF´s own systems but also other systems that directly affect the national defence capability can be better secured with the military cyber capabilities (Finnish Government, 2021). However, these systems are not defined in more detail in the report. It´s also worth noticing that the FDF protects mainly its own military systems. If a cyber attack is targeted to civilian infrastructure, it takes time to identify and prove the attacker as other state. Therefore, the importance of resilience in society as well as cooperation and information sharing with other authorities cannot be overlooked.

According to the Finnish Cyber Strategy, OCO can be used as a tool for political and economic coercion, and in a serious crisis as one means of influence alongside other traditional military means of force. (Turvallisuuskomitea, 2013) In this case, the actor is a military organization, which must be considered in terms of the potential risk of escalation.

The cyber domain is protected by increasing the threshold for different types of cyberattacks, for example by improving the detection and attribution ability of cyberattacks and the ability for countermeasures. Countermeasures can consist of, for example, law enforcement measures, diplomatic measures or active cyber countermeasures. (Turvallisuuskomitea, 2019)

3. Methodology and results

This study applies characteristics of cyber operations to the theory of cross domain deterrence. Content analysis (Puusa, 2021) was used as a research method so that factors could be separated from the investigated material in order to answer the research question.

The material concerning CDD and cyber deterrence was gathered from the abstract and citation database Scopus. The search was limited to the last ten years, since the perception of cyber phenomena have changed rapidly during past decades. After reaching saturation, some material was excluded due to being less relevant. The material concerning Finland was searched from the websites of Finnish Government and the FDF. The analyzed material contained five Finnish strategic documents, one handbook of Finnish military cyber operations, one US doctrine of cyber operations, five CDD articles and seventeen cyber deterrence articles.

During the first round of analysing, themes supporting the research question were defined as belligerence and cost-effectiveness of cyber operations and deterrence. Finnish cyber operations were investigated to create factors describing the types, functions and actors of cyber operations.

After the initial coding, in order to better understand the characteristics of military cyber operations, a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis (Pöyhönen, 2018) was carried out analysing cyber deterrence literature. The analysis focused on the internal strengths and weaknesses of military cyber operations used to secure Finland's sovereignty, as well as external opportunities and threats. The results are presented in the Table 1.

Based on the cyber deterrence literature, OCO can be executed cheaper and faster than other cyber operations. Since the attack can be planned beforehand at specific targets, it doesn´t require vast resources to execute (Rivera, 2015; Chen, 2017; Chen, 2018; Taddeo, 2018a) and covert operations are possible because of the attribution problem (Chen, 2017; Fischerkeller, 2017). This could create an opportunity with a surprise element and taking initiative.

OCO and DCO-RA are more belligerent in nature than the other cyber operation types, since the target is an opponent system (JP 3-12, 2018; Laari et al, 2019). Therefore, there is a risk of escalation (Schneider 2019). For managing escalation, in theory, scaling the attack intensity is possible (Leuprecht et al, 2019; Burton, 2018) and in an ideal situation both OCO and DCO-RA are repeatable (Mallick, 2021; Harknett & Smeets, 2022) and even reversible (Fischerkeller, 2017).

The advantage of active use of offensive cyber capabilities can also be seen as a weakness if too much of a state's cyber abilities are revealed and a foothold for the opponent system is lost (Schneider, 2019). There might also appear problems with attribution, speed, accuracy and repeatability (Mallick, 2021).

DCO-IDM include active measures for protecting the friendly cyberspace by tracing the origin of the attack and mitigating its effects on friendly networks. Along with C5O, these actions create the basis for deterrence by denial. If DCO-IDM is implemented with artificial intelligence and machine learning, a real-time ability to detect, and identify the attacker can be achieved. (Rivera, 2015) It´s worth noting, however, that in Finland military operations protect mainly the FDF`s cyber domain leaving out the rest of the society. It is possible for other authorities to ask for assistance for specific situations, but the process might take time.

C5O creates the basis for deterrence by denial in creating resilience, because the ability to recover mitigates the effects of cyberattacks. The focus is on the maintenance, management, disruption tolerance, system recovery and development of information systems and networks. The C5O should be understood as a continuous and long-term investment in the construction and development of cyber security. (Laari et al, 2019) In Finland, the FDF protects cyber domain and the resilience of the rest of society is divided with several public and private actors. There´s a risk of deficiencies in information sharing between military actors and other authorities.

Resilience is an important factor of deterrence by denial, but in cyberspace it also requires active means for isolating the attacker and mitigating its effects (Fischer, 2019). This includes an element of deception, which can be achieved by various technical means, such as honeypots or traps of malware that are launched when information is stolen (Wanic & Rowe, 2018). Together with DCO and C5O these passive and active effects can be achieved.

Table 1: SWOT analysis of Finnish cyber operations

Type	Purpose and target	Benefits	Disadvantages	Opportunities	Risks
OCO	Attacking aggressor state outside friendly cyberspace	Credibility, cost-effectiveness, speed	Loosing foothold, revealing capabilities	Gaining surprise and initiative	Escalation, uncontrolled effects, unrepeatability
DCO-RA	Retaliating aggressor actor outside the FDF cyber domain and assisting other authorities when requested	Credibility, cost-effectiveness, speed in FDF networks	Loosing foothold, revealing capabilities, military cyber operations concentrate on the FDF and could be slow on other friendly networks	Mitigating attacks, limiting and isolating of the impact	Escalation, unrepeatability
DCO-IDM	Protecting the FDF cyber domain and assisting other authorities when requested	Activity and anticipation	Inefficiency to focus on essential threats, military cyber operations concentrate on the FDF	Mitigating attacks, deceiving adversary	Lack in performance
C5	Protecting the FDF cyber domain and assisting other authorities when requested	Recovery	Insufficient alone, not feasible by military cyber operations only	Decreasing attack vectors	Cost-effectiveness, passivity, deficiencies in information sharing

After the SWOT analysis, the understanding was deepened with factors found in the CDD theory. The focus on the third round of coding was to define escalation risk and cost-effectiveness of cyber operations and preconditions to be met in order to achieve the desired effects as deterrents. Based on the analysis, a table was created to describe the nature and role of cyber operations as part of cross domain deterrence. The results are presented in Table 2.

From a deterrence point of view, some preconditions must be met before executing OCO. First, red lines should be clearly stated, so there are less chances of mistaking the consequences for hostile actions from the adversary´s point of view (Rivera, 2015). Second, national law and international agreements must be abided by for the OCO to be justified (Huskaj & Moradian, 2018; Rivera, 2015; Schneider, 2019; Mandel, 2017; Fischer, 2019; Wanic & Rowe 2018). Third, in order to be credible, demonstrations of cyber power must be made (Wanic & Rowe, 2018; Taddeo, 2018b). It should also be noted, that the use of other military capabilities could either amplify or moderate the effects of OCO (Fischerkeller, 2017).

The low cost of OCO is based on fact that the execution is fast and requires only little money or human resources compared to defending against an attack (Janczewski & Caelli, 2016). On the other hand, creating the foothold for the attack could take time and require a lot of preparations in the form of information gathering and building a technical capability.

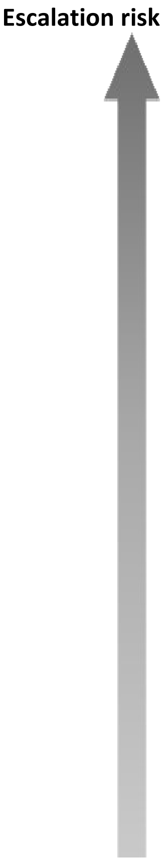
The DCO-RA differs from OCO in its retaliatory nature where OCO can be used in advance. DCO-RA offers means for deterrence by punishment in a milder form than OCO. Countermeasures are used to communicate to the attacker that the attack has been detected and it is possible to respond to it. (Laari et al, 2019)

DCO-RA requires successful attribution (Fischer, 2019) for the retaliation to be justified in the eyes of international actors. There is a risk of this taking too much time for the counteraction to be efficient. This risk can be countered in theory with automated countermeasures (Wanic & Rowe, 2018), that could be facilitated with artificial intelligence (Rivera, 2015; Taddeo, 2018b).

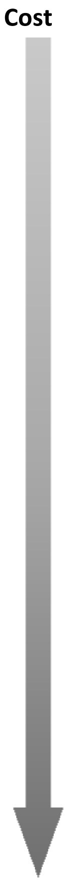
For the DCO-IDM to be successful, the friendly cyberspace needs to be monitored. For this, the FDF needs the cooperation of other domestic and international actors in terms of threat information sharing. If a friendly network outside the FDF needs assistant, for example in terms of threat hunting, there must be a request for help from other authorities. This might take time to execute.

Cyber resilience in Finnish society is built on several actors, including public and private actors as well as citizen (Turvallisuuskomitea, 2013). Therefore, the role of the FDF is minimal regarding any other than its own cyberspace. The military national defence capability is secured with C5O, but the society needs all the actors to cooperate in securing the critical infrastructure. The resilience needs a continuous strategy and efficient resources, that involves the whole society in building and maintaining it.

Table 2: Finnish military cyber operations as deterrents



Type	Objective	Deterrence	Preconditions	Benefits and opportunities	Disadvantages and risks
OCO	Attack	By punishment	Law, preparation of targets, continuous foothold, repeatability, signalling red lines	Credibility, cost-effectiveness, speed, gaining surprise and initiative	Loosing foothold, revealing capabilities, escalation, uncontrolled effects, unrepeatability
DCO-RA	Retaliation	By punishment	Law, attribution, signalling red lines	Credibility, cost-effectiveness, speed, mitigating attacks, limiting and isolating of the impact	Escalation, unrepeatability, loosing foothold of opponent system, revealing capabilities, military cyber operations concentrate on FDF
DCO-IDM	Defence	By denial	Surveillance, cooperation	Activity and anticipation, mitigating attacks, deceiving adversary	Lack in performance, inefficiency to focus on essential threats,



Escalation risk

Cost

Type	Objective	Deterrence	Preconditions	Benefits and opportunities	Disadvantages and risks
					military cyber operations concentrate on FDF
C5O	Resilience	By denial	Strategy, resources, continuity	Recovery, decreasing attack vectors	Cost-effectiveness, passivity, insufficient alone, not feasible by military cyber operations only

In the fourth round of the analysis, the gathered information was compared to "A Framework for Cross-Domain Strategies Against Hybrid Threats" by Sweijs, Zilincik, Bekkers and Meessen. The framework divides escalation options into five categories, which can be used in DIMEL (Diplomatic, Information including cyber, Military, Economic, Legal) model with each dimension. Categories are cooperation, persuasion, protection, coercion (including deterrence) and control, increasing in escalatory nature from the first to the last. (Sweijs et al, 2020) This framework is relevant to this study, because it draws to the theory of CDD extending the perspective beyond deterrence. It also addresses the modern threat environment with hybrid threats. For future research, the analysis performed in this paper can be utilized in future research focusing on the framework in its entirety.

This study investigated deterrence options in every dimension and the rest of the framework was excluded. Finnish cyber operations were included in the framework and examples were generated based on the previous analysis rounds. Table 3 sets out the proposal of how Finnish cyber operations could be used as a part of this framework with other dimensions for creating deterrence.

Table 3: Finnish cyber operations in "A Framework for Cross-Domain Strategies Against Hybrid Threats"

Dimension	General examples (Sweijs et al, 2020)	Example of support from dimension to cyber operations	Example support from cyber operations to dimension	CO type related
Diplomatic	Threatening diplomatic isolation in order to maintain the adversary's current behaviour, possibly with diplomatic allies.	Communicating the will to use offensive cyber capabilities and own resilience via strategic documents and official announcements of the state administration.	Demonstrations of offensive capabilities	OCO, DCO-RA, DCO-IDM, C5O
Information	Threatening retaliation through information warfare, counterintelligence	Information gathering and counterintelligence in physical and information domains in order to predict possible cyber attacks	Information gathering and counterintelligence in cyber domain	OCO, DCO-RA, Cyber ISR (Intelligence, Surveillance, Reconnaissance)
Military	Credibly established and communicated retaliatory capability.	Demonstrations of military capabilities	Demonstrations of offensive capabilities	OCO, DCO-RA
Economic	Threatening the use of sanctions/ supply manipulation/ price increase in order to maintain the target's current behaviour.	Sanctions with diplomatic allies targeting supply chains	Demonstrations of offensive capabilities and protecting own critical infrastructure	OCO, DCO-RA, DCO-IDM, C5O
Legal	Threats of legal sanctions to dissuade the adversary from breaking the rule. Alternatively, this includes threats of prosecution within one's domestic legal jurisdiction if a target does not accept one's demands.	Legal support for executing all types of cyber operations in predetermined conditions. Legal support for domestic and international cooperation and information sharing.	Carry out operations in accordance with the law, gathering forensic evidence to support attribution in case of cyber attacks	OCO, DCO-RA, DCO-IDM, C5O

4. Conclusions and future research

As a conclusion, it can be stated that cyber operations, especially C5 and defensive cyber operations, have a role in creating deterrence against threats occurring in or through the cyberspace. Offensive cyber operations work best as part of an overall deterrence that involves not only the use of armed force but also legal, political and, economic means. In order for an OCO to be worthy of being used as a deterrent, there must be a clearly demonstrable reason why this is done. Probably, in such a situation, the threat actor is already doing such provocative and damaging actions that a cyber operation alone is not enough to be used as a sufficient countermeasure, but it is also necessary to use military deterrent measures. At this stage, there may also be a limit as to whether it is purely a deterrence in question, or the prevention of an already starting crisis and the prevention of escalation.

For a small state, using cyber operations as a deterrent from the escalation and cost-effectiveness point of view is bipartite. On the one hand, OCO and DCO-RA might require less resources to implement, but they are also belligerent and could lead to escalation. On the other hand, DCO-IDM and C5 operations require a vast amount of resources to protect the civilian infrastructure and achieving sufficient resilience takes a lot of time, but these means are not escalatory in nature. For a small state´s perspective, it´s necessary to build resilience and profitable to develop offensive and retaliatory cyber capabilities.

In future research, the analysis formed in this article could be extended to include other small states and different ways of structuring cyber operations. To better understand the use of cyber capabilities as a deterrent, it is necessary to investigate the possibilities of states to build a credible deterrence in today's threat environment.

References

11.5.2007/551, (2007). *Laki Puolustusvoimista*, Finlex. https://www.finlex.fi/fi/laki/ajantasa/2007/20070551.

Arie, K. (2016) Complex Deterrence Theory and the Post-Cold War Security Environment, *NIDS Journal of Defense and Security*, No. 17, December 2016, pp. 21-39.

Burton, J., (2018). *Cyber Deterrence: A Comprehensive Approach?* Nato Cooperative Cyber Defence Centre of Excellence, Estonia 2018.

Chen, J. (2017). Deterrence and its Implementation in Cyber Warfare, in *ICCWS 2017 12th International Conference on Cyber Warfare and Security*, United states.

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

Coolsaet, R. (2004). Small States in World Politics: Explaining Foreign Policy Behavior. *Int Polit* 41, 284–285. https://doi.org/10.1057/palgrave.ip.8800051.

Finnish Government, (2021). *Government's Defence Report*, Publications of the Finnish Government 2021:80, Helsinki 2021, ISSN pdf: 2490-0966.

Fischer, M., (2019). The Concept of Deterrence and its Applicability in the Cyber Domain, in *Connections: The Quarterly Journal 18*, no. 1, 69-92. DOI: 10.11610/Connections.18.1-2.05.

Fischerkeller, M., (2017). Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies, *Survival*, 59:1, 103-134, DOI: 10.1080/00396338.2017.1282679.

Gartzke, E., Lindsay, R., (2017a). Thermonuclear cyberwar, *Journal of Cybersecurity*, Volume 3, Issue 1, March 2017, Pages 37–48. https://doi.org/10.1093/cybsec/tyw017.

Goetschel, L. (2000) Small States and the Common Foreign and Security Policy (CFSP) of the EU: A Comparative Analysis, *NRP42 Project-4042-044205 Final Report*, Berne, May 2000.

Hanska, J. (2019). Pelotetta vai pidäkettä? Deterrenssiteorian käytäntöä pienen valtion näkökulmasta. *Tiede Ja Ase*, 2019(1). https://journal.fi/ta/article/view/88681.

Harknett, R. & Smeets, M., (2022). Cyber campaigns and strategic outcomes, in *Journal of Strategic Studies*, 45:4, 534-567, DOI: 10.1080/01402390.2020.1732354.

Huskaj, G. & Moradian, E., (2018). Cyber Deterrence: An Illustration of Implementation, in *13th International Conference on Cyber Warfare and Security,* 8 – 9 March 2018, Washington, DC, USA.

Janczewski, L. & Caelli, W. (2016). Security of small countries: Summary and model in Janczewski, Lech and William Caelli (eds): *Cyber conflicts and small states*, UK, ISBN 978-1-4724-5219-1.

JP 3-0, (2017). *Joint Operations*, US Joint Chiefs of Staff.

JP 3-12*,* (2018). *Cyberspace Operations,* US Joint Chiefs of Staff.

Kerttunen, M. (2019). Beyond Punishment: Deterrence in the Digital Realm. *Connections*, 18(1/2), 61–68. DOI: 10.11610/Connections.18.1-2.04.

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.

Leuprecht, C., Szeman, J. & Skillicorn, B., (2019). The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity, in *Contemporary Security Policy*, 40:3, 382-407, DOI: 10.1080/13523260.2019.1590960.

Lindsay J., Gartzke E. (2017b). Cross-Domain Deterrence and Cybersecurity: The Consequences of Complexity, with Erik Gartzke, in *US National Cybersecurity: International Politics, Concepts and Organization*, ed. Damien van Puyvelde, Aaron F. Brantley (New York: Routledge, 2017). DOI: 10.4324/9781315225623.

Lindsay J., Gartzke E. (2019). Introduction: Cross-Domain Deterrence, From Practice to Theory, in Lindsay J., Gartzke E. (eds) *Cross-Domain Deterrence: Strategy in an Era of Complexity*, Oxford University Press, Oxford. https://doi.org/10.1093/oso/9780190908645.003.0001.

Mallick, P. (2021). *Deterrence Theory– Is it Applicable in Cyber Domain?* The Centre for Land Warfare Studies, Vivekananda International Foundation, New Delhi, ISBN: 978-93-91498-05-4.

Mandel, R. (2017). *Optimizing cyberdeterrence: a comprehensive strategy for preventing foreign cyberattacks.* Washington, DC : Georgetown University Press. ISBN: 9781626164123; 9781626164130.

Mazarr, M., Goodby, J. (2011). Redefining the Role of Deterrence, in Hoover Institution on War, Shultz, R., Drell, G. & Goodby, J. *Deterrence: Its past and future: Papers presented at Hoover Institution,* November 2010. Stanford, Calif.: Hoover Institution Press.

Morgan, P. (2003) *Deterrence Now*. Cambridge: Cambridge University Press (Cambridge Studies in International Relations). DOI: 10.1017/CBO9780511491573.

Puolustusministeriö, (2019). *Kyberpuolustuksen kehittämisen strategiset linjaukset*. ISBN: 978-951-663-069-7 pdf.

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

Pöyhönen, J. (2018). *SWOT-analyysin soveltaminen yrityksen kyberturvallisuuden tilannekuvan muodostamiseen*. Informaatioteknologian tiedekunnan julkaisuja, No. 58/2018, Jyväskylän yliopisto.

Radoman, J. (2018). *Small States in World Politics: State of the Art*. 179-200. 10.11643/issn.2217-995X182SPR101. DOI: 10.11643/issn.2217-995X182SPR101.

Rivera, J. (2015). Achieving cyberdeterrence and the ability of small states to hold large states at risk, in *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, 2015, pp. 7-24, DOI: 10.1109/CYCON.2015.7158465.

Schneider, J., (2019). Deterrence in and through Cyberspace, in *Cross Domain Deterrence*, Lindsay & Gartzke eds. https://doi.org/10.1093/oso/9780190908645.003.0005.

Sweijs, T., Zilincik, S. Bekkers, F. & Meessen, R. (2021). *A Framework for Cross-Domain Strategies*
Against Hybrid Threats, The Hague Centre for Strategic Studies, 2021.

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

Taddeo, M., (2018b). Deterrence and Norms to Foster Stability in Cyberspace. *Philos. Technol.* 31, 323–329 (2018). https://doi.org/10.1007/s13347-018-0328-0.

Toomse, R. (2015). *Defending Estonia in peace and war. Retaining a small state near aggressive neighbor by utilizing unconventional strategies.* Dissertations on social sciences, Tallinn University 2015.

Turvallisuuskomitea, (2013). *Suomen kyberturvallisuusstrategia*, ISBN: 978-951-25-2434-1 pdf.

Turvallisuuskomitea, (2019). *Suomen kyberturvallisuusstrategia 2019*, ISBN: 978-951-663-051-2 pdf.

Väyrynen, R. (1997). Small States: Persisting Despite Doubts in *The National Security of Small States in a Changing World*, edited by Efraim Inbar and Gabriel Sheffer, 41−77. London: Frank Cass.

Wanic, E. and Rowe, N. (2018). Assessing Deterrence Optinos for Cyber Weapons, in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 13-18, doi: 10.1109/CSCI46756.2018.00011.