Cyber Deterrence: An Illustration of Implementation

Gazmend Huskaj[1] and Esmiralda Moradian[2]
[1]Department of Military Studies, Swedish Defence University, Stockholm, Sweden
[2]Department of Computer and Systems Sciences, Stockholm University, Kista, Sweden
gazmend.huskaj@fhs.se
esmirald@dsv.su.se

Abstract: Cyber deterrence is a strategy employed to deter attackers from conducting cyber-attacks in the first place. However, several issues identified in this paper exist when implementing cyber deterrence. The findings show (1) non-existence of the deterrence strategy (2) no doctrine or decision competence to retaliate to an adversary, (3) the armed forces have no authority to retaliate when Swedish sovereignty in Cyberspace is threatened, (4) no norms or regulations exist concerning retaliation, (5) no clear governance on using offensive cyber capabilities, and finally, (6) no credibility in its cyber deterrence posture regarding how much Sweden is willing to sacrifice to protect its electoral system, which is a Swedish national interest. Therefore, this research investigates how cyber deterrence can practically be implemented in Swedish cyber security policy. So far, researchers generally focused on the human aspect of cyber deterrence. By using the case study research strategy and utilizing the Swedish electoral system as a case, this paper examines possibilities to merge the human dimensions of cyber security with the technological dimensions. Data collection is performed through documents studies and semi-structured interviews with experts in the area to identify cyber deterrence components. Further, a mathematical approach is discussed in the paper to express the relationship between an adversary and a deterrent depicting each of the actor's risk calculus. A result of the research work is performed in this paper, the deterrence components for Swedish cyber deterrence are proposed and risk calculus is performed. Moreover, measures to increase Swedish cyber deterrence posture are proposed the practical implementation of cyber deterrence in Swedish cyber security policy in order to deter attacks on the Swedish electoral system is demonstrated.

Keywords: cyber deterrence, cyber strategy, cyber policy, risk calculus, mathematical illustration, Swedish electoral system

1. Introduction

Cyber deterrence is a strategy employed to deter attackers from conducting cyber-attacks. Cyber-attacks can target any cyber-asset from any place in the world. Transnational in nature, they have evolved and become sophisticated, like Stuxnet that attacked the Natanz nuclear facility and the massive DDoS directed towards Estonia in 2007. "The attacks range from attacks to critical infrastructure, to political-related matters" (Mandel, 2017). The US Office of the Director of National Intelligence (ODNI, 2017) stated that another dimension of cyber-attacks targeting the US 2016 elections was discovered: attacks on key democratic leaders, the infrastructure that facilitates electronic voting, and their suppliers. These attacks were combined with influence campaigns. In Sweden, "threats to Swedish computer and networked information systems are real" (Wallin as cited by Hazianastasiou, 2017). Looking at cyber deterrence, Goodman (2010: 103) states that the theoretical foundation of cyber deterrence is laid, with several authors doing research in this area, especially on the human side. However, according to Jensen (2012), Alperovitch (2011), Lupovici (2011), Goodman (2010), and Taipale (2009) the existing research does not consider the interconnection of the human and technological dimensions of cyber deterrence. There is also a lack of information on how to implement cyber deterrence practically in Swedish cyber security policy by connecting the human and technological dimensions of cyber security.

2. Related work

Snyder (1960) defines six cyber deterrence components: base, means, amount, scope and "the object values and the credibility of a threat or promise" (Snyder, 1960). Snyder's (1961; 1960) and Dahl's (1957) mathematical illustration expresses that the relationship between an adversary and a deterrent can be used to quantify risk management by assessing the threat likelihood and impact. This research is based on Snyder's (1961) "mathematical illustration" and illustrates how cyber deterrence can be implemented practically in Swedish cyber security policy.

Illustrating this, Snyder (1961) assumes that each side "is able to translate and combine all of its own relevant values into a single numerical utility, that each can and does estimate probabilities for the other's moves, and that each acts rationally according to the principle of 'mathematical expectation'" (ibid). Assume four states, A, B, C, and D, where A represents the aggressor, D represents the deterrent and B and C are contested territories. In this first model, A has many ground forces while D has none. The contested territories of B and C have no forces and are allied to D. For the sake of the illustration, A has two moves, either use all forces to attack B, or

to not attack at all. D has also two moves: to retaliate with full force or do nothing, thus losing an ally, B. Then, Snyder (1961) adds the value of 100 for total war and notes that both the aggressor A and the deterrent D value B to 20.

Table 1 shows Snyder's (1961) illustration of A's and D's cost-gain estimates. "A estimates the probability of retaliation by D by attempting to guess D's payoffs and D's capacity to act rationally in accordance with them" (Snyder, 1961). A estimates that D will not retaliate because it is irrational. Moreover, A is not sure whether D will act rationally or irrationally. However, Snyder (1961) points out that A is not aware of how D estimates the consequences of war, nor how D valuates the consequences. A then believes that there is a one in 10 chance of retaliation by D. This does not deter A "because his expected value from attacking is greater than the expected value from not attacking" (Snyder, 1961). Calculating this, results:

$$0.10 \times (-100) + 0.90 \times (20) = 8$$

Although D cannot know A's expected value, he can probably say it is small and positive. D then assumes a probability of 0.60 for an attack and a 0.40 for a non-attack. "D's 'expected value' of -12 (probability of A's attack times D's losses with his best response) is a rough measure of D's degree of insecurity" (Snyder, 1961).

Table 1: The aggressor's and the deterrent's calculus. Source: Snyder, 1961

A's Calculus			D's Calculus		
Deterrer	Attack	Not Attack	Deterrer	Attack 0.60	Not Attack 0.40
Retaliate 0.10	-100	0	Retaliate	-100	0
Not Retaliate 0.90	+20	0	Not Retaliate	-20	0
Expected Value	+8	0	Expected Value	-12	0

3. Deterrence components

The deterrence components were initially defined by Dahl (1957), and then expanded by Snyder (1961), Goodman (2010) and Libicki (2016). According to Goodman (2010), deterrence components are sub-parts or elements of deterrence and consist of base, means, amount, scope, object values, credibility, thresholds and denial measures. When all components are implemented, a strong and effective deterrence strategy is defined. The lack of any of these components results in a weak and ineffective deterrence strategy.

Dahl (1957) states that base is the means that enables a capacity to affect others. In a Swedish context, based on the findings from the interviews, base includes alliances, capability, capacity, communication/signalling, detection, evidence, governance, guardians, legal, society, technology, system architecture, network communications, protocols, hardware, software, operating systems, databases, access control and standards. Snyder (1960) emphasizes that alliances enable the deterrent to increase its capacity to affect an adversary, and each member must have certain capabilities for deterrence to work. Examples include the detection, degradation and conduct of offensive cyber operations. An example of how capacity and capability are linked is the claim that "NATO's ballistic missile defence capacity will be an important addition to the Alliance's capabilities for deterrence and defence" (NATO, 2012).

Libicki (2016) and Goodman (2010) state that communication aims to inform adversaries of the consequences in the event that an adversary threatens an interest of the deterrer. To identify threats, detection is important. This can be done by using honeypots. Pfleeger (2015) points out that the results can be used as evidence, as a honeypot lures and monitors the adversary's tools, tactics and procedures. In 2017, Higgins reported that "a global research honeypot tracked … a large amount of reconnaissance traffic coming from Russian IP addresses."

The Swedish Code of Statutes (SFS, 1962) accentuates the fact that the legal landscape in Sweden regarding computer intrusions is low. Combined with the absence of capable guardians defending the electoral system, computer intrusions can affect society's trust in the electoral system. Therefore, understanding technology, its strengths, weaknesses, opportunities and threats is important to use as a base. To deter threats, Pfleeger (2015) proposes making attacks harder but not impossible. System architecture can "limit the information a port scan reveals about a network and its hosts and services" (Pfleeger, 2015).

Means is "the method by which the power base is brought to bear, for example, by threat, ultimatum, or force demonstration" (Snyder, 1960). In the Swedish context, the base according to Libicki (2016) can be used to

respond to cyber-attacks by exposing the adversary, responding economically, punishing, doing nothing or retaliating in several ways (cyber-to-cyber, cross-domain, proxy), explicit or implicit. Snyder (1960) states that amount can only be specified in conjunction with the means and the scope. "Scope is the range of potential actions by the other party which can be influenced by the threat or promise of applying the base" (Snyder, 1960). OWASP (2013) emphasizes that potential adversary actions affecting object values include, but are not limited to, reconnaissance-actions, spear-phishing, and man-in-the-middle attacks. "Object values are the values of the other party, which are subject to being decreased by the actual carrying-out of the threat or promise" (Snyder, 1960). Examples include cities, the financial system, the electrical grid, and telecommunications.

Credibility has been defined by several researchers, such as Snyder (1960), Schelling (1966), Goodman (2010), and Libicki (2016). Schelling (1966) points out the importance of credibility by highlighting the power and close-to-zealous intent a state must have in the interests of credibility. He takes the example of when the Soviet Union deterred the West from entering Hungary. "The Soviet Union was strong enough, and likely enough to react militarily, to make Hungary seem not worth the risk, no matter who might get hurt worse" (Schelling, 1966). A Western act of entering Hungary was within the Soviets' threshold of acts that result in retaliation. Thresholds distinguish acts that can result in retaliation from those that can be either deterministic or probabilistic. Libicki (2016) states that a deterministic posture is "if you do this, we will do that", therefore a probabilistic posture is "if you anger us enough by your behavior, we might strike back?"

Denial measures are "military forces that can block the enemy's military forces from making territorial gains" (Snyder, 1960).

4. Results and practical implementation of cyber deterrence in Swedish cyber security policy

Literature studies and interviews with Swedish policy and technology experts were performed. This resulted in requirements for cyber deterrence being identified and verified in this research. Text in quotation marks are direct quotes from the respondents.

The Swedish electoral system was used as a case to demonstrate the implementation of cyber deterrence in Swedish cyber security policy, connecting the human and technological dimensions of cyber security.

4.1 Swedish cyber deterrence policy components' requirements

The base in Swedish Cyber Deterrence policy consists of several means. Examples include alliances, capability, capacity, detection, evidence, governance, technology, standards, etc. According to the respondents, Sweden has limited capacity in relation to a greater adversary. Moreover, it is necessary to have the capability to detect, degrade and conduct offensive cyber operations for cyber deterrence to work. Targeting an adversary's communication infrastructure with the purpose of reducing their cyber-attack capability should exist. Furthermore, the results from the interviews clearly show that the development of an offensive cyber capability should include the ability to penetrate and deface adversarial systems by exploiting software flaws identified through passive means. Additionally, Sweden should communicate its cyber deterrence strategy by:

- Communicating that "to manipulate the electoral system is a violation on the UN charter".
- Communicating that all intrusion attempts on the electoral system will be exposed.
- Establishing a "Cyber Intelligence Alliance" with like-minded countries to increase each country's redundancy, capacity and deterrent posture. This sends signals such as "if you hit [Sweden], then you risk being hit from other directions".
- Conducting red-team exercises to communicate that Sweden possesses a certain cyber capability to show competence. This deters would-be attackers.

Detection is vital to expose threats to the electoral system. For example, tools detecting port scanning must exist. The resulting evidence, collected through intelligence, technical and/or forensic means, is elevated at the international level. No attribution is required and evidence through intelligence is sufficient.

Governance is linked to the will to retaliate. The offensive cyber capability raises the question of how it will be governed in case of cyber-attacks towards the electoral system. The police have a permanent mandate to use force required to solve the task while the armed forces do not.

Due to a lack of cooperation, norms or regulations have to exist stating that "if the circumstances are A, B, and C, then it's acceptable to use the active capability as retorsion towards a state actor". The Armed Forces as a guardian lack the authority to assert Swedish sovereignty in Swedish Cyberspace. Regulations SFS 1982:756 and SFS 2007:1266 instruct the Armed Forces. However, these regulations should be modernised and include Cyberspace and the Cyber domain to give the Armed Forces the authority to be a very capable guardian of the electoral system. This would increase Swedish capacity to guard the electoral system and use the entire weapons arsenal. Asserting the right to self-defence in the event of an attack is a form of retaliation. However, retaliation on behaviours such as intrusion on computer systems is limited, and this is valid for the electoral system; there is no penal code regarding crimes against democracy. One way forward is a penal contingency with the collection name "crimes against democracy", where intrusion attempts towards the electoral system trigger parts of the penal code regarding sabotage and national security. This results in heavier penalties. Finally, an adversary allowing its agents to act or perform computer intrusion attempts towards the electoral system from their territory should be held accountable through the Friendly Relations principle. Such incidents need to be communicated to society in order to keep trust in the electoral system.

The networks, hardware and software in each voting machine need to be secured. The electoral system architecture should be designed based on the threats to be managed and evaluated before development and deployment. Network communications should be protected by considering the principles of confidentiality, integrity and availability. Electoral information is highly confidential and its integrity crucial to ensure trust in the results. Therefore, encryption and secure transport protocols are required. However, interview results and literature review findings show that there are not many secure protocols. This means that it is necessary to either use current secure protocols, develop new secure protocols, or put other safeguards in place to protect electoral information being transferred through the application, transport, network and data-link layers.

The electoral system should be audited by a third party and the design should take into account the assumption that Sweden manages the environment. The hardware supporting the electoral system should be in a physically separated server park with redundancy, or, considering the idea that the cloud is the future, in a private cloud.

There is no preferred operating system (OS). Weaknesses in UNIX, Linux and Windows should be considered. Consequently, the OS should be secured and tested. Security solutions can be developed from scratch or be built into an existing OS following a secure development lifecycle. Developers must have a security clearance and no information about what type of OS is released to the public. Software that is used for vote collection, managing, storing and retrieving electoral information must be developed using a secure development lifecycle. Developers must have a security clearance. This means the database that is utilized should be tested through security tests. Access to the system shall always follow the 'need-to-know' principle. Voters must be verified in an equal way as it is done in the manual election, and when voting, they should use at least two-factor-authentication.

Standards and best practices should be followed when designing the electoral system. The results are identified risks that need to be managed. Risk management is done by employing layers of security controls, also known as defence in depth. It makes harder for an adversary to affect the confidentiality and integrity of electoral information. Only evaluated cryptographic algorithms according to BSI in Germany, Common Criteria components, and only developed in Sweden should be used. Third party assurance certificates such as "ISAE3402, SOC1 or 2" should also be considered. Auditable standards need to be independently validated. Threats should be analysed and threat levels should be defined. Furthermore, the security requirements need to be evaluated.

Means include detecting and exposing adversary intrusion attempts, retaliating cyber-to-cyber, cross-domain or through proxy. The mean to detect and expose adversary intrusion attempts targeting the electoral system should be done at an early stage. Cyber-to-cyber retaliation can be to penetrate, degrade or deface adversarial systems. Penetrating an e-mail system is exploited by revealing the adversary's e-mail. Defacement is exploited by revealing the information to mass media as soon as possible and both acts create embarrassment. Penetrating closed systems indicating "Sweden is here" increases the credibility of Swedish cyber capabilities. The adversarial infrastructure that is being targeted should not be revealed.

Cross-domain retaliation using sanctions is an option when there is no mandate to use cyber-attacks or physical attacks. However, Sweden has no doctrine and decision competence to retaliate. The will could be mobilised, but not at such speed during a cyber-attack.

The Swedish threat to retaliate can be cyber-to-cyber and cross-domain, but not through proxy. Retaliation through proxy loses its effect. Cyber-attacks as responses to cyber-attacks targeting the electoral system should not be revealed, because this enables their denial. Counter-attacks should target the state adversary over the individual because Sweden cannot handle such kinds of public debates with the current system. The threat of retaliation is implicit and contains the element of uncertainty. Therefore, a strategy of uncertainty is preferred where Sweden reserves the right to use all means available. These means, the threat of retaliation, with the credibility to penetrate closed systems, are important to get into the adversary's decision-making process. They can deter an adversary and they bind adversarial resources to manage the results of the created embarrassment.

Influencing the adversary's potential actions targeting the electoral system is also about influencing his behaviour. According to the respondents, Sweden will not accept any type of behaviour that affects the electoral system, obstructs or changes the outcome of an election.

The Armed Forces need the authority to protect Sweden's sovereignty in cyberspace. Authorisation can be given by amending the "regulation on the Armed Forces' interventions in the event of violations of Sweden's territory under peace and neutrality" (the IKFN Regulation) to protect Swedish cyberspace by using all means necessary. Then, according to the experts, a credible body that targets and degrades adversarial object values, such as telecom-switches, would exist. Targeting and degrading an adversary's object values would take place when the adversary targets the electoral system.

The respondents stated that Sweden has no doctrine and decision competence to retaliate to an adversary. Additionally, the experts claimed that the Armed Forces have no authority to retaliate, there are no norms or regulations, and Sweden has a limited capacity in relation to a greater adversary. Therefore, Sweden lacks the credibility to threaten a greater adversary targeting the electoral system with retaliation. Sweden has to resolve these issues to be credible in its cyber deterrence posture.

The experts point out that Sweden cannot state where the thresholds are because there is no support. It is likely that a probabilistic posture is more in line. Sweden reserves the right to use all means available, how and when are not discussed. However, according to interviewees, some thresholds have been mentioned; there is no tolerance of any form of behaviour or action that aims to affect the electoral system, obstructing or changing the outcome of an election.

The interviewees point out that denial measures include honeypots, procuring voting machines through non-regular procurement procedures, building the system thoroughly with several sensors, and using dark fibre. This is communicated to inform the adversary and the citizens that the voting machines and the electoral system are hardened. Communicating these measures denies the adversary the benefits of carrying out cyber-attacks and show confidence in the electoral system.

4.2 Practical implementation

The risk calculus on the electoral system illustrates the necessary measures required to be in place. The risk calculus is based on Snyder's (1961) approach.

All values in the following calculus are assumed values. Assume that A is the "adversary" and D is the "deterrer". A is a greater nation while D is a smaller nation. Based on previous cases, it is likely that A's cost-gain estimates, or expected value for cyber-attacks, are higher than refraining from conducting cyber-attacks. It is assumed that A's likelihood to conduct cyber-attacks to affect the outcome of an election is very likely, or 0.9 on a scale from zero (0) to one (1).

The value of the electoral system to D is 100 and to A is 90, or higher, depending on the gains A estimates to achieve. D is not expected to gain any value from the electoral system other than to maintain it. A gains value by affecting the electoral system resulting in a political candidate pro to A's cause. Therefore, A has the advantage of more gains. A needs to assess the likelihood that D will retaliate by attempting to assess D's payoffs and capacity. Retaliation is expected through media-exposure and possible sanctions (cross-domain), and A assesses the cost of retaliation to 9, because A will not lose territory, cities, or any other object values. This calculus is depicted in Table 2.

All-out war is unlikely and is thus not considered. Both A and D are rational. For convenience reasons, the first model covers only a generalised cyber-attack.

Table 2: A's risk calculus and trade-offs

	Adversary	
Deterrer	Attack	Not Attack
Retaliate 0.9	-9	0
Not retaliate 0.1	90	0
Expected Value	0.9	

What happens if A, the greater nation, puts all capacities to use and is confident of succeeding in installing a political leader who is not of the political establishment? A asserts this confidence by rating the value of D's electoral system to 200. This calculus is depicted in Table 3.

Table 3: A's risk calculus and trade-offs, and the expected value

	Adversary	
Deterrer	Attack	Not Attack
Retaliate 0.9	-9	0
Not retaliate 0.1	200	0
Expected Value	11.9	

Based on previous cyber-attacks targeting the 2016 US election, D should by now expect and assess cyber-attacks targeting the electoral system as very likely, or 0.9 on a scale zero (0) to one (1). This calculus is depicted in Table 4.

Table 4: D's assessment of his own deterrent posture

	Adversary	
Deterrer	Attack	Not Attack
Retaliate	0.9	0.1
Not retaliate	-100	0
Expected Value	-90	

D's estimate of the likelihood of 0.9 that A will conduct cyber-attacks targeting D's electoral system is a measurement of D's deterrent posture.

D's expected value of -90 is a rough measure of his insecurity. D can increase the deterrence posture by physically separating the electoral system networks from the Internet.

Now, consider the same reasoning where Sweden is the deterrer D, and A is a greater nation. Again, all values are assumed.

The US case shows the inherent value of the electoral system. D values the electoral system to 100. As above, it is likely that A's cost-gain estimates, or expected value for cyber-attacks targeting the electoral system, are higher than not conducting the attacks. It is assumed that A's likelihood to conduct cyber-attacks to affect the outcome of an election is very likely, or 0.9 on a scale from zero (0) to one (1). The value of the electoral system to D is 100 and to A is 90, or higher, depending on the gains A estimates to achieve. D is not expected to gain any value from the electoral system other than to maintain it. A gains value by affecting the electoral system resulting in a political candidate pro to A's cause. Therefore, A has the advantage of more gains. A needs to assess the likelihood that D will retaliate by attempting to assess D's payoffs and capacity. Retaliation is expected through media-exposure and possible sanctions (cross-domain), and A assesses the cost of retaliation to 9, because A will not lose any territory, cities, or any other object values. All-out war is unlikely and thus is not considered. Both A and D are rational. This model covers A's risk calculus for each attack-and-response and the resulting expected value for A. For convenience reasons, D's estimated losses with each move-and-response are symmetrical. This calculus is depicted in Table 5.

Table 5: D's calculus on D's estimated losses with each move-and-response

	Adversary		
Deterrer	Not Attack	Cyber-attacks	Influence-campaigns
No response	0	-100	-100
Cyber-to-Cyber (C2C)	0	-80	-80

	Adversary		
Deterrer	Not Attack	Cyber-attacks	Influence-campaigns
Sanctions	0	-90	-90
Media-exposure	0	-95	-95
Likelihood of A's moves		0.5	0.5
Expected Value (EV) C2C	0	-40	-40
EV Sanctions	0	-45	-45
EV Media-exposure	0	-47.5	-47.5

D assesses that A will conduct cyber-attacks and influence-campaigns to the electoral system. D estimates the likelihood of the attacks to 0.5.

If D does not respond to either cyber-attacks or influence-campaigns, then D's estimated losses are 100. This means that the adversary has succeeded in installing a political candidate who is pro to A's cause.

If D responds cyber-to-cyber, then D has a slight chance of affecting A's cyber-attacks and influence campaigns, but not much.

If D responds with sanctions, and considering that these do not have an immediate effect, then D has a minor chance of affecting A's cyber-attacks and influence campaigns.

If D responds with media-exposure, and the adversary is not affected because the adversary already controls all media within his own territory, then D has a very minor chance of affecting A's cyber-attacks and influence campaigns.

Therefore, D can increase its deterrence posture by using the following measures:

- Increasing awareness amongst political candidates and their staff and auditing their computer and information systems for weaknesses.
- Classification of the electoral system as a national interest and critical infrastructure.
- Development of doctrine and decision competence to retaliate in cyberspace.
- Authorising the Armed Forces to retaliate when Swedish sovereignty in Cyberspace is threatened.
- Developing norms and regulations.
- Clear governance on using cyber capabilities.
- Increasing credibility through a willingness to sacrifice to protect the electoral system, democracy and Sweden in general.

5. Conclusions and future work

This study has conducted risk calculus and identified the components in Swedish cyber deterrence policy: base, means, amount, scope, object values, credibility, thresholds, and denial measures. Each component has multiple sub-components: cyber alliances increase capacity and deterrence; detection measures expose threat activity; legal issues must be resolved; a government cloud, secure communications, protocols and secure software must be developed. In addition, each sub-component includes reasoning if, for example, retaliation should be cyber-to-cyber, cross-domain, or through proxies. The implications of each course of action are also discussed. Finally, measures to increase deterrence posture are defined.

This research demonstrated how cyber deterrence could be implemented practically in Swedish cyber security policy. The research resulted in the following:

- performing risk calculus,
- identifying deterrence components in Swedish cyber security policy,
- identifying measures to increase cyber deterrence posture.

This study opens up for research in several areas including:

- The components of cyber deterrence.

- Secure system architectures and secure network protocols that may provide deeper studies in cyber deterrence.
- Increasing reliance on systems and in society to mitigate influence campaigns to protect the electoral system and to maintain society's trust in it.
- Developing norms and regulations to decide what is acceptable behaviour regarding cyber-attacks targeting another nation's electoral system.
- Policy that considers the social and technological aspects of cyber by bridging the gap between policymakers and technology-oriented people
- How to use offensive cyber capabilities towards which adversarial targets.

References

Alperovitch, D. (2011) "Towards Establishment of Cyberspace Deterrence Strategy", in C. Czosseck, E. Tyugu, T. Wingfield (eds.), 2011 3rd International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, Estonia, pp 87-94.

Dahl, R. (1957) "The Concept of Power", [online], The University of North Carolina at Chapel Hill, https://www.unc.edu/~fbaum/teaching/articles/Dahl_Power_1957.pdf.

Goodman, W. (2010) "Cyber Deterrence: Tougher in Theory than in Practice?", *Strategic Studies Quarterly,* Fall, Vol 4, No. 3, pp 102-135.

Hazianastasiou, S. (2017) "Sverige utsatt för allvarliga cyberattacker -Försvarets radioanstalt: 10 000 fall i månaden", [online], Norrtelje Tidning, http://www.norrteljetidning.se/inrikes/sverige-utsatt-for-allvarliga-cyberattacker-forsvarets-radioanstalt-10-000-fall-i-manaden.

Higgins, K.J. (2017) "Russia Top Source of Nefarious Internet Traffic", [online], Darkreading, https://www.darkreading.com/threat-intelligence/russia-top-source-of-nefarious-internet-traffic-/d/d-id/1328255.

Jensen, E. (2012) "Cyber Deterrence", *Emory International Law Review*, Vol 26, No. 2, pp 773-824.

Libicki, M. (2016) *Cyberspace in Peace and War*, Naval Institute Press.

Lupovici, A. (2011) "Cyber Warfare and Deterrence: Trends and Challenges in Research", *Military and Strategic Affairs*, Vol 3, No.3, pp 49-62.

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

NATO. (2012) "Deterrence and Defence Posture Review", [online], North Atlantic Treaty Organization, http://www.nato.int/cps/en/natohq/official_texts_87597.htm.

ODNI. (2017) "Assessing Russian Activities and Intentions in Recent US Elections", [online], Office of the Director of National Intelligence, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

OWASP. (2013) "Top 10 2013-Top 10", [online], OWASP Foundation, https://www.owasp.org/index.php/Top_10_2013-Top_10.

Pfleeger, C.P. and Pfleeger, S.L. (2015) *Security in Computing*, Prentice Hall.

Schelling, T. C. (1966) *Arms and Influence*, Yale University Press.

SFS 1962:700. "Brottsbalk (1962:700)", [online], Justitiedepartementet, http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700_sfs-1962-700#K4.

SFS 1982:756. "Förordning (1982:756) om Försvarsmaktens ingripanden vid kränkningar av Sveriges territorium under fred och neutralitet, m.m. (IKFN-förordning)", [online], Försvarsdepartementet, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-1982756-om-forsvarsmaktens_sfs-1982-756.

SFS 2007:1266. "Förordning (2007:1266) med instruktion för Försvarsmakten", [online], Försvarsdepartementet, http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20071266-med-instruktion-for_sfs-2007-1266.

Snyder, G. (1960) "Deterrence and Power", *The Journal of Conflict Resolution*, Vol 4, No. 2, June, pp 163-178.

Snyder, G. (1961) *Deterrence and Defense*, Princeton Legacy Library.

Taipale, K.A. (2009) "Cyber-deterrence", *Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization*, IGI Global, 2010.