Erno Pajala

SITUATION AWARENESS AND CYBER KILL CHAIN WHEN RUSSIAN CYBER OPERATORS HACKED THE DEMOCRATIC NATIONAL COMMITTEE

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Pajala, Erno
Tilannetietoisuus ja cyber kill chain- viitekehys, kun venäläiset kyberoperaattorit hakkeroivat demokraattien kansallisen komitean
Jyväskylä: Jyväskylän yliopisto, 2020, 30 s.
Tietojärjestelmätiede, kandidaattitutkielma
Ohjaaja: Marttiin, Pentti

Tämä kandidaatintutkielma on tutkimus Yhdysvaltojen demokraattinen kansallinen komitean reagoinnista ja toimenpiteistä, kun Venäjä hakkeroitui komitean tietoverkkoihin. Tutkielma tarkastelee nimenomaisesti sitä, tekikö komitea oikeat toimenpiteet.

Venäjä hakkeroi Yhdysvaltojen demokraattipuolueen vuosina 2015 ja 2016 ennen Yhdysvaltojen presidentinvaaleja. Tapahtumia on analysoitu käyttäen kyberturvallisuusviitekehystä yhdistettynä tilannetietoisuusteoriaan. Tutkimus on toteutettu kirjallisuuskatsauksena.

Tutkielma käsittelee kyberoperaatioita keskittyen kyberpuolustukseen sekä tilannetietoisuuteen päätöksenteon tarkastelussa, tietojärjestelmätieteen näkökulmasta. Tilannetietoisuus on tärkeä osa päätöksentekoa, joka voi olla helposti puutteellista monista tekijöistä riippuen.

Tarkasteltuja tapauksia on kolme. Ensimmäinen alkoi 2015 kesällä, kun Venäjä hakkeroi demokraattisen kansallisen komitean tietoverkot. Toinen tapaus koskee jo mainittua Venäjän hakkerointia, mutta tilannetietoisuus muuttui merkittävästi toisessa tapauksessa. Kolmas tapaus alkoi 2016, kun toinen kyberoperaattori Venäjältä hakkeroi demokraattisen kansallisen komitean tietoverkot ja alkoi varastamaan tiedostoja kyseisistä verkoista.

Tämä tutkielma tarkastelee, millaisia kyberoperaatioita Venäjä teki Yhdysvaltojen 2016 presidentinvaaleissa. Toimittiinko tilanteessa viitekehyksen mukaan ja oliko toiminta tilannetietoisuusteorian pohjalta oikeaa? Mainittuja aiheita ei ole tutkittu tilannetietoisuuden näkökulmasta. Lähdemateriaali kostuu osittain viranomaisten raporteista ja monipuolisista kansainvälisten mediatalojen uutisista, sillä akateemista tutkimusta aiheesta on niukasti.

Asiasanat: kybersodankäynti, tiedustelu, tilannetietoisuus, päätöksenteko

ABSTRACT

Pajala, Erno
Situation awareness and Cyber Kill Chain when Russian cyber operators hacked Democratic National Committee
Jyväskylä: University of Jyväskylä, 2020, 30 pp.
Information Systems, Bachelor's Thesis
Supervisor: Marttiin, Pentti

This thesis is a research on the United States Democratic National Committee's reaction and actions when Russia hacked the Committee's networks. Thesis examines precisely, did the Committee conduct the correct actions.

Russia hacked the United States Democratic National Committee in 2015 and 2016 before the United States presidential election. The incidents are analyzed using cyber security framework, combined with situation awareness theory. Research is done as literary review.

Thesis addresses cyber operations focusing on cyber defense and situation awareness in decision making from information system science's viewpoint. Situation awareness is an important part of decision making that can easily be lacking depending on different elements.

Three incidents are examined. The first incident started in the summer of 2015 when Russia hacked the Democratic National Committee's networks. The second incident regards the already mentioned incident but situation awareness changes significantly in the second incident. The third incident started in the spring of 2016 when different a cyber operator from Russia hacked the Democratic National Committee's networks and started to steal documents from those networks.

This thesis examines what kind of cyber operations Russia conducted regarding the 2016 United States presidential elections. Were actions done according to cyber security framework and were reactions correct according to situation awareness theory. Mentioned subjects have not been studied from situation awareness viewpoint. Source material is partly based of government reports and from diverse selection of international media publishers' news articles, because academic research was found only sparsely.

Keywords: cyberwarfare, exploitation, situational awareness, decision making

FIGURES

TABLES

CONTENT

ABBREVIATIONS, ACRONYMS AND INITIALISMS

APT	**Advanced Persistent Threat**
CKC	**Cyber Kill Chain**
DCCC	**Democratic Congressional Campaign Committee**
DNC	**Democratic National Committee**
FBI	**Federal Bureau of Investigation**
FSB	**Federal Security Service of the Russian Federation**
FSO	**Federal Protective Service of the Russian Federation**
GRU	**The Main Directorate of the General Staff of the Armed Forces of the Russian Federation**
NSA	**National Security Agency**
OPCW	**Organisation for the Prohibition of Chemical Weapons**
SVR	**Foreign Intelligence Service of the Russian Federation**

1 INTRODUCTION

> Richard Clarce said: "If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked."
> (ZDNet, 2002).

Cyber threat is rated higher in the U.S. Intelligence community than global terrorism (Kello, 2013). Many countries conduct cyber operations against each other and against private and nongovernmental organizations. Russia's GRU tried to attack OPCW and their investigation into the usage of chemical weapons in Syria (Government of the Netherlands, 2018). In September 2019, Russia tried to access NATO and its partners by phishing (*www.securelist.com*, 2019). Israel attacked Iran as a revenge for Iran's attempt to disrupt Israel's water network by attacking Iran's shipping (The Washington Post, 2020). Israel has even used conventional warfare against hackers from the terrorist organization Hamas (Forbes, 2019). The focus of this study is on how organizations react when they become the target of cyberspace operations.

What are cyberspace operations, what should be the appropriate response when targeted by them? Cyberspace operations are defensive and offensive operations conducted in cyberspace (Joint Chiefs of Staff, 2018). Reaction depends on which stage the cyber attack is (Lockheed Martin, 2015). Lockheed Martin is one of many security houses and cyber security operators that has come up with so called "Cyber Kill Chain". It is a framework to counter cyber attacks. The Cyber Kill Chain has 7 stages in which the defender can stop the adversary. (Lockheed Martin, 2015).

In the study decision making is analyzed through Endsley's situation awareness theory. Situational awareness, according to Endsley (1995) is the basis for decision making. With complete situational awareness performance is better when the subject, tackling the problem has capabilities in said the situation. There are many human errors that can cause failures in decision making, but Endsley lists three that affect the situational awareness part of decision making. These are failure to perceive information, inability to understand and link perceived data according to operators' goals and insufficient situational awareness. (Endsley, 1995).

Russia has four different government agencies conducting cyber operations (Estonian Foreign Intelligence Service, 2018). Two of them concentrate on internal security and two of them operate outside of Russia. GRU is the one whose agents are mostly former Spetsnaz and are the ones behind Skripal (BBC, 2019) poisoning and the brazing hacking attempt of the OPCW files on Syria's use of chemical weapons (Government of the Netherlands, 2018). SVR is the one that is thought to have poisoned former Russian spy Alexander Litvinenko (Ocunus, 2006). GRU has APT28 and SVR APT29 as their cyber operators (Estonian Foreign Intelligence Service, 2018).

APT28 and APT29, in 2016, hacked the US Democratic National Committee's , the Democratic Congressional Campaign Committee's networks and Hillary Clinton's presidential campaign's emails (Mueller, 2019). This study is focused on the Democratic National Committee networks hacking, because there is more information about it. This study shows how important situation awareness and correct cyberspace actions are for cybersecurity.
The research question is formed as follows:

> *How did the Democratic National Committee react, and did they perform the correct actions when Russia hacked their networks?*

This study is done as a literary review. The sources used are books, government reports, white papers, news articles, and academic articles. The focus was heavily on newspaper articles and on white papers since, there were no studies made on cyber attacks or exploitation. Source selection was based on their novelty, reverence and relevance. Sources are searched from Google and from Google Scholar. The authors of the articles came from many different fields of science. Sources were collected using such words as "cyber exploitation", "cyber espionage", "Russian cyber operations", "cyber warfare", "APT", "cyber security", "situation awareness", "kill chain", and combinations of the above.

The first concept in the study is cyberspace operations followed by Lockheed Martin's Cyber Kill Chain framework and Russia's cyber operators. To analyze decision making, Endsley's situation awareness theory is relevant for this study.

The study will give the reader more insight on cyberspace operations, Cyber Kill Chain, situation awareness theory and on how Russia conducts cyber operations. The reader will gain an understanding of how to base decisions on situational awareness and what to do when under cyber exploitation. This is done from the perspective of information system sciences, combining the security angle with the organization angle.

2 CYBER OPERATIONS

The term cyberspace was invented by science fiction writer William Gibson in 1984 to mean a digital space for communication (Reveron, 2012). Cyberspace is a place for cheap and easy ways to disrupt competition (Whyte, 2016). Cyber operation (cyberspace operations) missions can be divided into two branches, external cyberspace operations and internal cyberspace operations (Joint Chiefs of Staff, 2018). These in turn can be divided into offensive and defensive cyberspace operations. Defensive operations can be further divided into two parts, defensive network operations and defensive cyberspace operations (Williams, 2014). Williams has offensive and defensive cyberspace operations as separate entities. The Joint Chiefs of Staff of the US Army, in their JP3-12 publication, go more in depth on the topic of cyberspace operations than Williams. In JP3-12, defensive operations also conduct offensive operations as a response actions for defensive purposes (Joint Chiefs of Staff, 2018). Offensive operations include cyber attacks and cyber exploitation. Cyber attacks, for them to be defined as such, must produce physical destruction or loss of life. Cyber exploitation is defined as gaining access to a cyberspace network to enable future operations and to gain intelligence. (Joint Chiefs of Staff, 2018). Cyber defense consists of detecting the attack, forming situation awareness and making defensive decisions (Saydjari, 2003).

Cyber attacks can be more expensive or damaging than conventional warfare (Marr, 2019). For example Iran's cyber attack against Israel's water network could have been expensive or damaging (The Washington Post, 2020). With dispersed facilities, an airstrike or ground assault must be divided to attack all the targets or choose the most valuable target. With a cyber attack, a dispersed network can be attacked all at once. (Marr, 2019). Cyber attacks can affect politics and Russia tried to influence United States 2016 elections by hacking voting machines (Mansfield-Devine, 2018).

Table 1 Terms and definitions of cyberspace operations according to Joint Chiefs of Staff (2018)

Term	Definition
Cyberspace	A global in the information environment consisting of connected networks of information technology infrastructure and data.
Cyberspace attack	Actions in cyberspace to create harm in cyberspace or in the physical world.
Cyberspace defense	Actions in cyberspace to defeat threats that have already breached or threaten to breach cyberspace security.
Cyberspace exploitation	Actions in cyberspace to gain advantage for operation or to gain intelligence.
Cyberspace security	Actions in cyberspace to protect networks and prevent unauthorized access, exploitation or damage to networks.

In its JP3-12, the Joint Chiefs of Staff (2018) describes cyber exploitation as cyber operation in which the operator enters the cyberspace and conducts operations in said cyberspace without getting noticed. Cyber exploitation can have the same elements as the attack itself, but it turns into a cyber attack when the operator knows that their actions will be noticed during the operation or sometime after. (Joint Chiefs of Staff, 2018).

Wortham (2011) speaks of cyber attack and cyber exploitation as different entities with similar attributes of entry and execution. Libicki (2017) uses the term cyber espionage as the prelude to cyber attack in same way that cyber exploitation is used. Different sources differentiate descriptions of cyber exploitation making it clear that the taxonomy for the term is imperfect. Cyber exploitation does not always lead to a cyber attack, but the problem is that it is perceived as a prelude to one (Lindsay & Kello, 2014). Banks (2017) talks of cyber espionage as a way of spying but cyber exploitation as more broad term to actually exploit the target's network and data in the network. According to Gupta and Joshi (2012) differences between cyber attack and cyber exploitation are in the objectives of the operation and in legality around them.

Online anonymity helps the actors to evade detection and retaliation (Lindsay, 2013) and keep cyber exploitation from turning into a cyber attack. Knowing who has accessed the network is a difficult technical problem making cyber exploitation harder to track than conventional spying (Banks, 2017).

2.1 Cyber Kill Chain framework

Lockheed Martin's Cyber Kill Chain was published in 2011 (Hutchins et al., 2011). Other models include FireEye's Kill Chain Model that was published in 2015 (FireEye, 2015) and Mitre's MITRE.ATTACK that was published in 2017

(Mitre, n.d.-a). Lockheed Martin's kill chain was the first cyber kill chain published and was a known framework when the Democratic National Committee's networks were hacked. FireEye's and Mitre's kill chains are based on Lockheed Martin's Cyber Kill Chain, which is the most used one of these. For this reason, Lockheed Martin's Cyber Kill Chain framework is used in this study.

The Cyber Kill Chain framework is a model for the identification and prevention of cyber intrusions activity (Lockheed Martin, 2015). It is based on the US military's kill chain tactic to find, fix, track, engage, and assess (Kiwia et al., 2018). Weapon manufacturer Lockheed Martin created the Cyber Kill Chain framework in 2011 as part of their Intelligence Driven Defense model. Cyber kill chain models mentioned earlier are all similar and based on Lockheed Martin's Cyber Kill Chain.

The Cyber Kill Chain has seven steps (figure 1). The defender can stop the attacker at any point in the Cyber Kill Chain (Lockheed Martin, 2015) and each step is crucial (Yadav & Rao, 2015). There are also three follow-up measures for to better cyber defense. These are analysis, reconstruction and resilience. (Lockheed Martin, 2015). The fourth step in the Cyber Kill Chain is exploitation. The term exploitation in this context is different from cyber exploitation mentioned before. In the Cyber Kill Chain exploitation is exploiting vulnerability to gain access (Kiwia et al., 2018), where cyber exploitation as a cyberspace operations is to gain advantage in the future or to gain intelligence (Joint Chiefs of Staff, 2018).

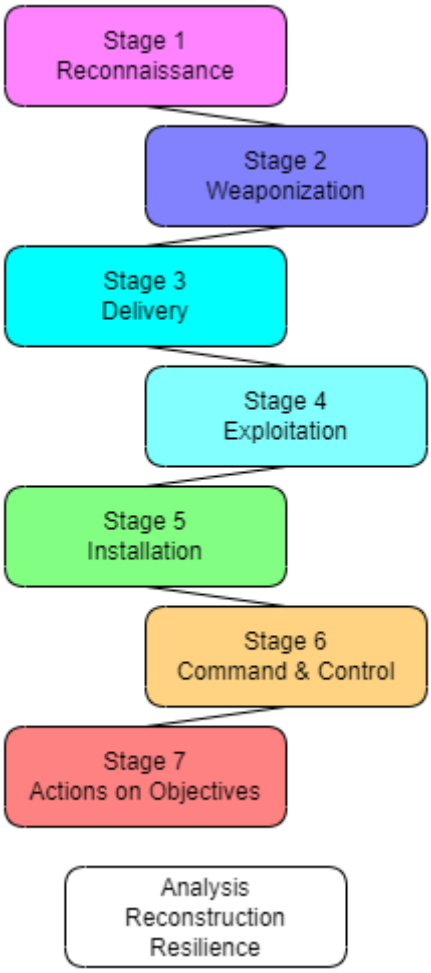

FIGURE 1 Lockheed Martin's Cyber Kill Chain (Lockheed Martin, 2015)

The seven steps Cyber Kill Chain (figure 1) are described as follows (Lockheed Martin, 2015):

Stage 1 is Reconnaissance. In this stage adversary tries to find access to target's network by conducting research and defender tries to discover the attacker's operations.

Stage 2 is Weaponization. This is the staging phase for the adversary. For the defender, this phase is essential. Weaponization cannot itself be detected, but e.g. malware can be analyzed in the defender's system if found.

Stage 3 is Delivery. This is when the adversary launches the operation by delivering the malware to the target. This is the defenders most important part of the kill chain in terms of preventing the attack.

Stage 4 is Exploitation. In this stage of the Cyber Kill Chain, the adversary gains access to the target. The defender can try to stop this phase by increasing user awareness and by other means that create more a secure information technology environment.

Stage 5 is Installation. In this stage, the adversary can install a backdoor or other means to gain a beachhead within to the defender's system. The defender can try and detect the installation of malware in their system or network.

Stage 6 is Command & Control. In this stage the adversary's malware tries to enable remote access to manipulate the victim. This is the defender's last change to prevent the attacker's operation.

Stage 7 is Actions on Objectives and it is the last stage. In this stage the adversary gets what it was after and the defender can analyze what has happened to them and then remedy their network. (Lockheed Martin, 2015).

2.2 Russia's cyber operators

Despite some debate regarding whether, Russia did in fact interfere in the U.S. election of 2016, there is proof that Russia was behind the attack using its APTs Fancy Bear and Cozy Bear (Mueller, 2019). Without a coordinated attack (The New York Times, 2016b). These two go by many names and APTs are part of Russian intelligence agencies SVR and GRU (figure 2).

Russia has four different security agencies that conduct cyber operations (figure 2). Of these operators, FSO and FSB focus more on defense and SVR and GRU on offence. SVR and GRU conduct more operations outside of Russia.

It is hard to identify where the hackers are from (Greenberg, 2019). Seals (2019) explains the reason for so many names. Different cybersecurity firms make up their own names for the operators. There are some names that are reserved for the operators of certain countries, panda for China, cat for Iran, lotus for Vietnam and bear for Russia. The use of numbers is that before the researcher are sure who the operator is they need some identification for the APT. (Threatpost, 2019).

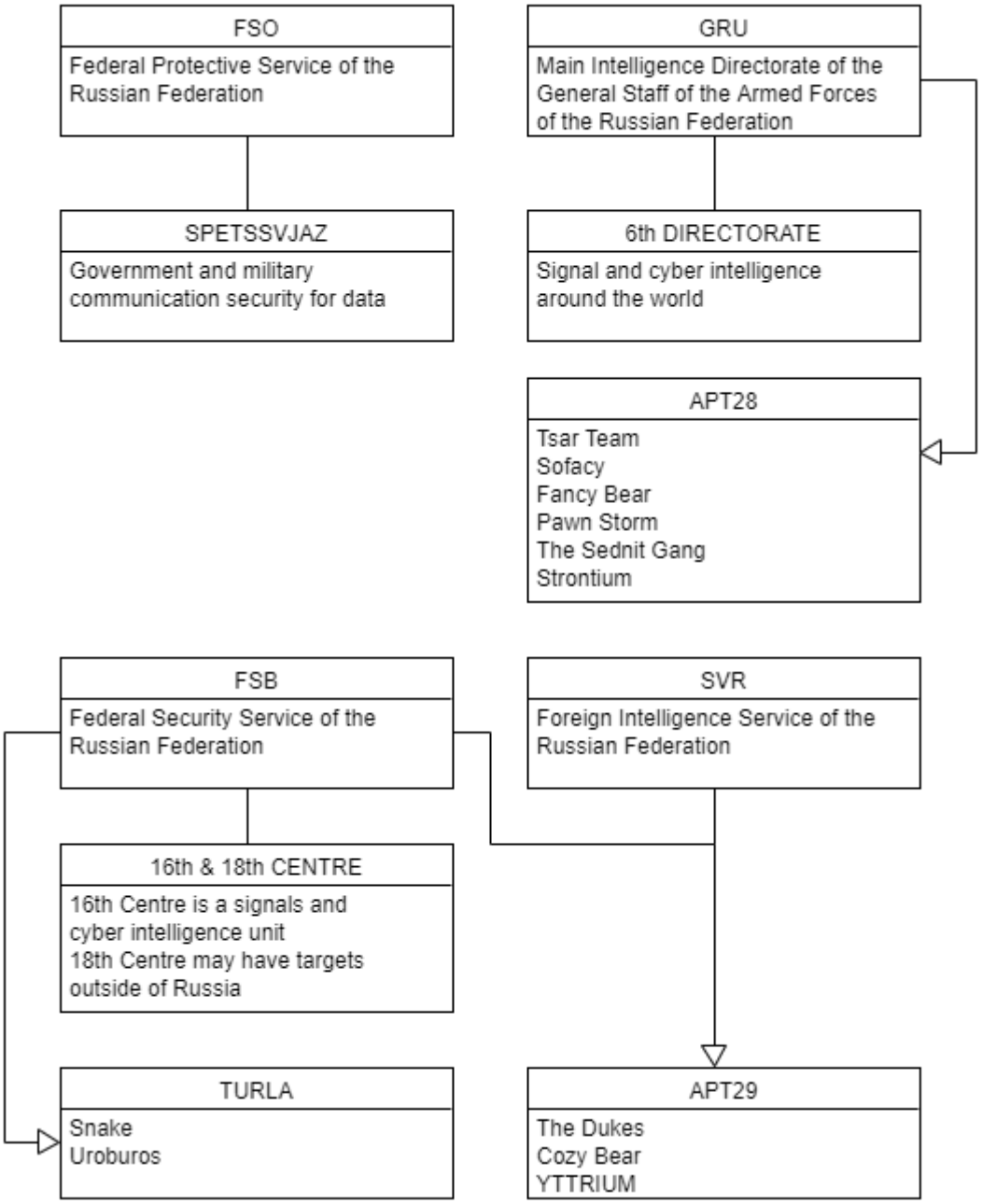

FIGURE 2 Russian cyberspace operators according to Estonian Foreign Intelligence Service (2018), Mitre (2019) & National Cyber Security Centre (2018)

2.2.1 The Main Directorate of the General Staff of the Armed Forces of the Russian Federation

GRU is the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Reuters, 2018). It answers to the chief of general staff and to the defense minister. It operates as a spy organization, cyber operator and as a military unit. (Reuters, 2018). GRU's 6th Directorate conducts signal and cyber intelligence as a more conventional unit. APT28 under GRU conducts hacking operations (figure 2).

2.2.2 Foreign Intelligence Service of the Russian Federation

SVR is the Foreign Intelligence Service of the Russian Federation (The Russian Government). It is led by the Head of the Foreign Intelligence Service and over-seen by the President of the Russian Federation. (The Russian Government). SVR is the civilian version of GRU and operates as a spy organization and as a cyber operator (The Moscow Project, 2018). APT29 operates under SVR and conducts its cyber operations (figure 2).

3 SITUATION AWARNESS THEORY

Situation awareness supports decision making and with situation awareness a person knows what is happening, what will happen and what actions they can perform (Koistinen, 2011). According to Endsley (1995) situation awareness is a state of knowledge that is achieved through situational assessment. Situation awareness creates the basis for decision-making and understanding the situation. Without accurate or complete situation awareness, decision makers cannot make right decisions. The situation awareness model consists of 5 actions (figure 3) and situational awareness itself of three levels (figure 4). An operator's goals and expectations, talents and operations complexity with system performance affect how well the operator goes through the situation awareness model. (Endsley, 1995). Endsley's situation awareness theory provides this thesis with a good and easy way to understand situation awareness from an academic perspective.

3.1 Situation awareness models

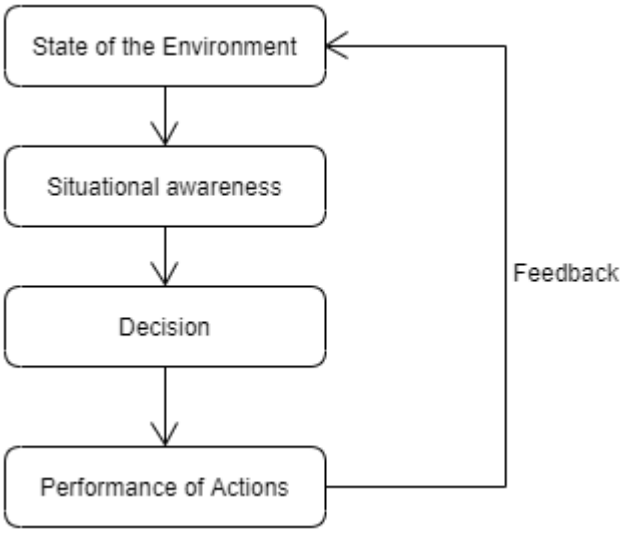

FIGURE 3 Situation Awareness Model by Endsley (1995)

Situation awareness theory's levels include state of environment, situational awareness, decision and performance of actions (Barford et al., 2010). Communication is important factor for situation awareness when it is formed by a team (Seppänen et al., 2013). Situation awareness model has person's individual factors and system factors that influence formation of situation awareness (Endsley, 1995). Automation is part of situation awareness and functions as a tool to help the operators situational awareness, decision-making and performance of actions (Endsley, 1995). However, automation can make the situation worse, according to Danks & Danks (2013) by escalating through an automated response from the attacker. Person's abilities and personal experiences influence situation awareness. (Endsley, 1995). Inexperience in cyber defense of the defender creates advantages for the adversary in a cyber attack (Dutt et al., 2013). With less experience lower level of situation awareness will be gained (Endsley, 1995).

Cyber situation awareness needs sensory data and understanding of that data (Saydjari, 2003). Barford et al. (2010) discuss the limitations of cyber situation awareness. They argue that there are fundamental differences between cyber situation awareness and physical situation awareness systems, physical systems relying on sensors and signals. Barford et al. (2010) say that signal processing could be used i.e. for network traffic analysis. There is a gap in the mental model of the analysis and capability of existing cyber situation awareness tools. (Barford et al., 2010).

3.2 Situation awareness levels

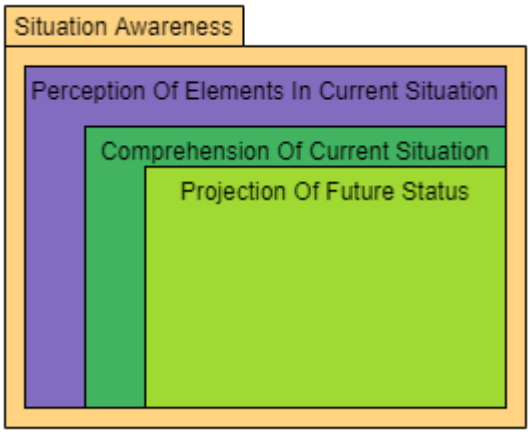

FIGURE 4 Situation Awareness levels from Endsley (1995) Situation Awareness Model

Situation awareness has three levels (figure 4). Level 1 situation awareness is achieved by perceiving the status, attributes and dynamics of elements in the environment (Endsley, 1995). Level 2 situation awareness is achieved with comprehension of the situation based on elements from level 1. Level 3 and final phase of situation awareness is achieved with level 1's elements and level 2's comprehension with the ability to project future actions of the elements in the environment. (Endsley, 1995).

4 ANALYSIS

Russian access to Democratic National Committee networks was gained in July 2015 (Office of the Director of National Intelligence, 2017) and ended on the 13th of July 2016 (Permanent Select Committee on Intelligence, 2017a). First SVR's APT29 started their cyber exploitation within Democratic National Committee networks (Nederlandse Omroep Stichting, 2018). In March 2016 GRU's APT28 got access to some of Hillary Clinton's presidential campaign team's emails (Mueller, 2019). In April, APT28 started their cyber attack by stealing thousands of documents from the Democratic Congressional Campaign Committee and Democratic National Committee networks (CrowdStrike, 2020). APT29 and APT28 conducted their operations separately and unaware of each other's cyber exploitation and attack (Nederlandse Omroep Stichting, 2018).

Table 2 Russia's hacking incidents of US Democratic party, situation awareness of the hacked party according to Endsley's theory (1995) and correct measures according Cyber Kill Chain framework (Lockheed Martin, 2015).

Incident	Reaction	Correct Cyber Kill Chain framework measure	Was performed	References
1. In July 2015 APT29 access DNC networks.	No reaction, Hacking not noticed. No SA.	Exploitation, Actions on Objectives	No	CrowdStrike (2020) Nederlandse Omroep Stichting (2018) (Lockheed Martin, 2015)

2.	In September 2015 NSA alert DNC that they are being hacked by APT29	Target informed of hacking. Does not believe callers legitimacy. Lacking SA.	Actions on Objectives	No	Nederlandse Omroep Stichting (2018) The New York Times (2016) Endsley (1995) Lockheed Martin (2015) (Mueller, 2019) Permanent Select Committee on Intelligence (2017b)
3.	In April 2016 Dutch intelligence alert NSA of DNC servers being hacked by APT28 and noticed also by DNC tech-support	Hacking started in early in April and was notified in 28th. Committee created to tackle what data was accessed, how and how to stop it. CrowdStrike hired. Attacker identified. SA level 3 reached.	Actions on Objectives	Yes	Nederlandse Omroep Stichting (2018) The New York Times (2016) Lockheed Martin (2015) CrowdStrike (2020) Endsley (1995) (Mueller, 2019)

4.1 Incident 1

In the first incident in this analysis, APT29 hacked the Democratic National Committee networks. In July 2015 APT29 accessed Democratic National Committee networks and maintained that access till June 2016 (Office of the Director of National Intelligence, 2017). US intelligence were informed of this hacking by Dutch intelligence already in the summer of 2015 (Nederlandse Omroep Stichting, 2018), but the Democratic National Committee was informed about suspicious activity in their computer network only in September 2015 by the FBI (CrowdStrike, 2020). Democratic National Committee had not noticed any suspicious activity in their network before then, and were not informed by FBI or NSA who knew of APT29's access already in July 2015. (CrowdStrike, 2020).

Because of this lack of knowledge, Democratic National Committee could not have had any situation awareness during this time. To have any level of situation awareness one needs to have some perceived information of the ele-

ments of the environment (Endsley, 1995). Therefore, not having any level of situation awareness, Democratic National Committee could not move to other parts of the situation awareness model. Without situation awareness no decisions or actions could be performed. (Endsley, 1995). All blame for lack of situation awareness does not fall on Democratic National Committee, but more on the US Government and the NSA and the FBI, who did not inform Democratic National Committee.

Democratic National Committee had no situation awareness in the situation so they could not perform any actions needed to counter APT29's hacking. The Cyber Kill Chain stages where Democratic National Committee could have stopped APT29 were stage 4 Exploitation and stage 6 Command and Control. These stages are chosen for closer examination because stage 4 is in this case is the first one where the Democratic National Committee realistically could have reacted in these circumstances, as stage 4 contains preventative actions. Stage 6, which contains malware analysis, is the last possibility to react to the hacking, because in this case for it did not lead to an attack. Correct procedures of stage 4 of which many are preventative actions like network user awareness and endpoint hardening measures (Lockheed Martin, 2015) are the ones that could have prevented the hacking. The attacker tries to get network users to open malicious emails (Lockheed Martin, 2015), which is preventable with training on how to use email securely. Stage 6 includes actions to detect the attacker by malware analysis, aiming to prevent or detect the attacker in the network (Lockheed Martin, 2015).

4.2 Incident 2

Incident 2 is a separate incident because the Democratic National Committee's situation awareness changes in it substantially. This change in situation awareness makes examination of incident 2 different from incident 1 and enables different stages from Cyber Kill Chain.

In September 2015, the FBI called the Democratic National Committee but was transferred to the Democratic National Committee's help desk and from there to Democratic National Committee's IT director (Permanent Select Committee on Intelligence, 2017b).The IT director, who did not know who or what 'The Dukes' were, googled it and then went through system logs, but did not find anything suspicious in the Democratic National Committee networks (The New York Times, 2016b). The FBI called the Democratic National Committee between September and December at least monthly and Democratic National Committee tech-support installed a new firewall in January (Permanent Select Committee on Intelligence, 2017b). According to CrowdStrike (2020) APT29 was not noticed in the Democratic National Committee computer network from July 2015 till 28th of April 2015 and had access to Democratic National Committee's computer network till June 2015.

Democratic National Committee has some perceived elements of the environment. These elements are as follows: who had accessed to Democratic National Committee networks and what they should do (Permanent Select Committee on Intelligence, 2017b). In the first call the FBI asked the Democratic National Committee's IT director to look for certain web traffic in Democratic National Committee networks. According to the IT director they found one article about the Dukes and searched their network for possible adversaries but did not find anything (Permanent Select Committee on Intelligence, 2017b). The FBI gave very redacted information that was, according to the IT director, quite obscure regarding the timing of possible hacking events (Permanent Select Committee on Intelligence, 2017b). Even with these elements of perception and the Democratic National Committee tech-team's limited knowledge of cyber security they do not have level 1 situation awareness. They did not have all the elements they needed to detect their adversary, having found only one article about them. They did not know if the adversary had in fact accessed their networks and they did not know when this possible cyber exploitation might have started. They did not have level 1 of situation awareness so they could not comprehend the current situation; without comprehension they could not project any possible further actions (Endsley, 1995).

The Democratic National Committee had some situation awareness but not enough to actually counter APT29's cyber exploitation at this time. APT29 was in stage 7 Actions and Objectives of the Cyber Kill Chain when the Democratic National Committee's tech team did not have any knowledge of their adversary or the adversary's cyber exploitation. In stage 7, the defender can try to detect lateral movement in their networks and try to capture package activity (Lockheed Martin, 2015). The Democratic National Committee tech team tried to detect movement in their network but with limited situation awareness they were unable to do so.

4.3 Incident 3

Incident 3 was conducted by APT28. APT28 accessed Hillary Clinton's presidential campaign team's emails and Democratic National Committee and Democratic Congressional Campaign Committee networks (Mueller, 2019). This analysis focuses on the hacking of Democratic National Committee networks and not on Democratic Congressional Campaign Committee networks or Clinton's presidential campaign team's email hacking, due to the availability of information on the hacking of the Democratic National Committee networks.

APT28 started its cyber attack on Democratic National Committee networks on the 22nd of April, almost immediately after it had gained access to the networks (Mueller, 2019). Dutch intelligence again informed US intelligence of APT28 actions (Nederlandse Omroep Stichting, 2018). On the 28th of April, Democratic National Committee's tech team noticed with their new firewall an unauthorized activity in Democratic National Committee networks (Permanent

Select Committee on Intelligence, 2017b). They pieced together the FBI's warnings and this incident, and realized they are actually under cyber attack (The New York Times, 2016b). The tech team had also noticed some phishing emails that were sent to Democratic National Committee members, but those emails were either not delivered to recipients or were not opened in Democratic National Committee's case (Permanent Select Committee on Intelligence, 2017b). Democratic National Committee formed a committee on the 29th of April to address the situation and figure out what data was accessed, how it was accessed and how to stop it (The New York Times, 2016b). On the 30th of April, the Democratic National Committee contacted CrowdStrike and on May 1st CrowdStrike started their investigation and identified APT28 and APT29 as the adversaries (CrowdStrike, 2020). On the 13th of July, Democratic National Committee networks were remediated (Permanent Select Committee on Intelligence, 2017a) and CrowdStrike and the Democratic National Committee informed the FBI that APT28 and APT29 had been in Democratic National Committee networks (CrowdStrike, 2020).

Situation awareness in incident 3 is at level 3 situation awareness of Endsley's framework (1995). Level 1 is achieved by knowing that the adversary, in this case APT28, exists. This is an element from Endsley's (1995) perception of elements and makes the tech team aware of their situation. Level 2 is achieved by understanding the impact of the cyber attack and the FBI's previous warnings. The tech team comprehended the situation and its impact on Democratic National Committee networks (Endsley, 1995). Tech team informed Democratic National Committee leadership and started to search for more suspicious activity in Democratic National Committee networks. The Democratic National Committee formed a committee and decided to hire CrowdStrike to investigate this cyber attack. These combined with levels 1 and 2 of situation awareness form highest form of situation awareness level 3 to Democratic National Committee. They could then project what was likely happen to the elements in their environment (Endsley, 1995).

With their achieved level of situation awareness the Democratic National Committee, with the help of CrowdStrike, could and did perform the correct measures of the Cyber Kill Chain's stage 7 Actions on Objectives (Lockheed Martin, 2015). Committee forming was a projection of future actions according to Endsley's situation awareness theory (Endsley, 1995). By forming the committee and understanding what data was stolen, they started to do damage assessment (Lockheed Martin, 2015). The collaboration with CrowdStrike allowed for establishing a response playbook. The tech team detected unauthorized suspicious movement in their network. By hiring CrowdStrike, the Democratic National Committee got forensic agents to endpoints for rapid triage. With these actions, the Democratic National Committee as a defender realized four out of five actions from the Cyber Kill Chain (Lockheed Martin, 2015).

4.4 Incident summary

The Democratic National Committee got their networks hacked twice by two different Russian cyberspace operators APT28 and APT29 (Mueller, 2019). When APT29 accessed their networks they did not notice any suspicious activities, and first knowledge of this came from the FBI months later (Permanent Select Committee on Intelligence, 2017b). Information given by the FBI was obscure and red tape prevented smoother collaboration with the Democratic National Committee and the FBI (Permanent Select Committee on Intelligence, 2017b). The NSA was the first organization in US to hear about possible hackings, but they are not mentioned after that (Nederlandse Omroep Stichting, 2018). There were no mentions of NSA involvement after this. APT29's cyber exploitation became known only when APT28 accessed the Democratic National Committee's networks and their actions were noticed by the Democratic National Committee's tech team (Mueller, 2019). APT28 started a full cyber attack, stealing as many documents and as much data as they can (The New York Times, 2016b). They were able to do this for almost a month in the Democratic National Committee networks, and even longer in those of the Democratic Congressional Campaign Committee and Hillary Clinton's presidential campaign team (Mueller, 2019). United States government would have been able to counter these cyber attacks better, but Obama administration did not make appropriate responses (CNBC, 2020). Obama administration did eject 35 Russian agents from the United States (The New York Times, 2016a). This thesis focused on only cyberspace operations against the Democratic National Committee.

5 CONCLUSION

Did the Democratic National Committee perform correct actions from Lockheed Martin's Cyber Kill Chain frameworks standpoint? Lacking situation awareness, they could not, but with fully realized situation awareness they did. Using Endsley's situation awareness theory and Lockheed Martin's Cyber Kill Chain framework this study was able to analyze the Democratic National Committee's actions when they were hacked.

Endsley's situation awareness theory has been around since 1995 but it is still relevant. It is used as basis for many situation awareness studies. Using Endsley's theory gave this study the conceptual tools for analyzing a person's or organization's situation awareness from an academic perspective. Situation awareness theory is heavily, in its own examples, military focused, but with enough familiarization one can utilize it in many ways. In this thesis, it was applied to cyber operations.

Lockheed Martin's Cyber Kill Chain is the most used when countering cyber adversaries. It was the first and all others are based on it. The Cyber Kill Chain outlines and actions for defending against cyberspace operations. A problem with the Cyber Kill Chain framework is that in all the incidents in this thesis, the adversary had already accessed the network, so each time the stage to perform was stage 7 Actions on Objectives. Adversaries can be stopped in all the stages of Cyber Kill Chain but in every incident, the adversaries were noticed in stage 7. It can be argued that stage 4 Exploitation is a stage which could counter all possible intrusion with its preventative actions.

The Democratic National Committee's organization situation awareness was non-existent in incident 1, heavily lacking in incident 2, but in incident 3 it was well formed. This shows that if situation awareness is achieved, correct actions can be performed from the Cyber Kill Chain framework's standpoint. If situation awareness is incomplete or only partial, one cannot perform correct actions. The analysis in this thesis showed that, communication is a significant part of situation awareness. Communicating well is key to the formation of situation awareness. Due to the FBI's poor communication with the Democratic National Committee, Russian cyber operators got more time to operate.

Literature on the subject of this thesis was hard to find. There are not many academic studies on cyber operations. Many sources were from cyber security organizations, newspapers and from government reports. The lack of academic studies on cyberspace operations is alarming. Numerous reports about cyber operations are classified and not published. The implications of this are tremendous. Academics cannot study and analyze them, which has created a knowledge vacuum in cyberspace operations studies.

The impact of cyberspace operations on society, governments and the economy is huge. The effect on politics is enormous as seen in the 2016 US presidential election. Russia started endorsing Trump after APT28's access to Democratic National Committee and Democratic Congressional Campaign Committee networks and Hillary Clinton's campaign's emails. Russia even tried to influence the election by hacking voting machines. The impact of cyberspace operations on anything cannot be diminished. cyberspace operations effects everything.

Future research on cyberspace operations is needed. There needs to be academic consensus on how cyberspace operations are conducted so there can be better and more academic frameworks on how to counter it. Taxonomy is another problem. Terms are made by different organizations and taxonomies overlap. For example, cyber exploitation can mean spying, reconnaissance, intelligence gathering or taking advantage of accessed network in cyberspace. The effect cyber operations on the world needs to be studied further. Many studies focus on how to conduct operations in certain environments or on how cyberspace operations have evolved, but more research needed on the potential impacts of cyberspace operations.

This thesis adds to information system sciences by analyzing the impact of technologies on organizations and analyzes use of technology from the perspective of both individuals and organizations. In today's ever-changing world and ever-changing cyber environment, understanding cyberspace operations and how to react to them is critical because cyberspace affects everything.

REFERENCES

Banks, W. (2017). Cyber espionage and electronic surveillance: Beyond the media coverage. *Emory L.J.*, *66*(513), 513–525.

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P., Ou, X., Song, D., Strater, L., Swarup, V., Tadda, G., Wang, C., & Yen, J. (2010). Cyber SA: Situational awareness for cyber defense. *Advances in Information Security*, *46*, 3–13. https://doi.org/10.1007/978-1-4419-0140-8_1

BBC. (2019, June 28). *Skripal poisoning: Third Russian suspect "commanded attack" - BBC News*. https://www.bbc.com/news/uk-48801205

CNBC. (2020). *Obama response to 2016 Russian meddling had many flaws: Senate report*. https://www.cnbc.com/2020/02/06/obama-response-to-2016-russian-meddling-had-many-flaws-senate-report.html

CrowdStrike. (2020, June 5). *Our Work with the DNC: Setting the record straight*. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Danks, D., & Danks, J. H. (2013). The moral Permissibility of automated responses during cyberwarfare. *Journal of Military Ethics*, *12*(1), 18–33. https://doi.org/10.1080/15027570.2013.782637

Dutt, V., Ahn, Y. S., & Gonzalez, C. (2013). Cyber situation awareness: Modeling detection of cyber attacks with instance-based learning theory. *Human Factors*, *55*(3), 605–618. https://doi.org/10.1177/0018720812464045

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, *37*(1), 32–64. https://doi.org/10.1518/001872095779049543

Estonian Foreign Intelligence Service. (2018). International Security and Estonia 2018. In *International Security and Peacebuilding*. https://doi.org/10.2307/j.ctt20061cg

FireEye. (2015). *Technology in Action*. 1–25.

Forbes. (2019, May 6). Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First. *Forbes*. https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#2a33c575afb5

Government of the Netherlands. (2018). *Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW | News item | Government.nl*. https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw

Greenberg, A. (2019). *Sandworm*. Doubleday.

Gupta, K. D., & Joshi, J. (2012). Methodological and Operational deliberations in Cyber attack and Cyber exploitation. *International Journal of Advanced*

Research in Computer Science and Software Engineering Research, *2*(11), 385–389.

Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *6th International Conference on Information Warfare and Security, ICIW 2011*, *July 2005*, 113–125.

Joint Chiefs of Staff. (2018). *Joint Publication 3-12 Cyberspace Operations*.

Kello, L. (2013). Security policy in the The Meaning of the Cyber Revolution. *International Security*, *38*(2), 7–40. https://doi.org/10.1162/ISEC_a_00138

Kiwia, D., Dehghantanha, A., Choo, K. K. R., & Slaughter, J. (2018). A cyber kill chain based taxonomy of banking trojans for evolutionary computational intelligence. *ArXiv*, *27*, 394–409.

Koistinen, M. (2011). *Tilannetietoisuus ja tilannekuva operatiivisessa liikenteenhallinnassa*. Aalto University.

Libicki, M. (2017). The coming of cyber espionage norms. *International Conference on Cyber Conflict, CYCON*, *2017-June*, 1–17. https://doi.org/10.23919/CYCON.2017.8240325

Lindsay, J. R. (2013). *Security Studies Stuxnet and the Limits of Cyber Warfare*. https://doi.org/10.1080/09636412.2013.816122

Lindsay, J. R., & Kello, L. (2014). *Correspondence: A Cyber Disagreement*. https://doi.org/10.1162/ISEC_c_00162

Lockheed Martin. (2015). *Gaining the Aavantage Applying Cyber Kill Chain® Methodology to Network Defense*.

Mansfield-Devine, S. (2018). Hacking democracy: abusing the Internet for political gain. *Network Security*.

Marr, C. (2019). Cyberwarfare and Applied Just War Theory: Assessing the Stuxnet Worm through Jus ad Bellum and Jus in Bello. *SPICE: Student Perspectives on Institutions, Choices and Ethics*, *14*(1), 2.

Mitre. (n.d.-a). *ATT&CK for Enterprise Introduction | MITRE ATT&CK®*. Retrieved December 6, 2020, from https://attack.mitre.org/resources/enterprise-introduction/

Mitre. (n.d.-b). *MITRE ATT&CK® EVALUATIONS*. Retrieved May 24, 2020, from https://attackevals.mitre.org/APT29/

Mueller, R. (2019). Report On The Investigation Into Russian Interferece In The 2016 Presidential Election. *U.S Depratment Of Justice*, *1* of *2*(March), 1–198. https://www.justice.gov/storage/report.pdf

National Cyber Security Centre. (2018). *Indicators of Compromise for Malware used by APT28*. *October*, 1–8.

Nederlandse Omroep Stichting. (2018, January 25). *Dutch intelligence first to alert U.S. about Russian hack of Democratic Party | Nieuwsuur*. https://nos.nl/nieuwsuur/artikel/2213767-dutch-intelligence-first-to-alert-u-s-about-russian-hack-of-democratic-party.html

Ocunus. (2006, December 7). *Russian Agency "Led Poison Plot."* https://web.archive.org/web/20070928004314/http://www.ocnus.net/cgi-bin/exec/view.cgi?archive=106&num=26989

Office of the Director of National Intelligence. (2017). Background to "Assessing Russian Activities and Intentions in Recent US Elections ": The Analytic Process and Cyber Incident Attribution Background to " Assessing Russian Activities and Intentions in Recent US Elections ": The Analytic Process and Cyber. *Office of the Director of National Intelligence*, *January*, 1–25.

Permanent Select Committee on Intelligence. (2017a). *Interview of: Shawn Henry*.

Permanent Select Committee on Intelligence. (2017b). *Interview of: Yared Tamene Wolde-Yohannes*.

Reuters. (2018). *What is Russia's GRU military intelligence agency? - Reuters*. https://www.reuters.com/article/us-britain-russia-gru-factbox/what-is-russias-gru-military-intelligence-agency-idUSKCN1MF1VK

Reveron, D. S. (2012). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Georgetown University Press.

Saydjari, O. S. (2003). Cyber Defense : Art To Science. *Communications of the ACM*, *46*(9).

Securelist. (2019). *APT trends report Q3 2019 | Securelist*. https://securelist.com/apt-trends-report-q3-2019/94530/

Seppänen, H., Mäkelä, J., Luokkala, P., & Virrantaus, K. (2013). Developing shared situational awareness for emergency management. *Safety Science*, *55*, 1–9. https://doi.org/10.1016/j.ssci.2012.12.009

The Moscow Project. (2018). *Russia's Three Intelligence Agencies, Explained - The Moscow Project*. https://themoscowproject.org/explainers/russias-three-intelligence-agencies-explained/

The New York Times. (2016a). *Obama Strikes Back at Russia for Election Hacking- The New York Times Obama Strikes Back at Russia for Election Hacking*. https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html?smprod=nytcore-ipad&smid=nytcore-ipad-share1/6https://nyti.ms/2hwS8pA

The New York Times. (2016b). *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.* https://nyti.ms/2hBJis3

The Russian Government. (n.d.). *Foreign Intelligence Service - The Russian Government*. Retrieved December 6, 2020, from http://government.ru/en/department/112/

The Washington Post. (2020). *Officials: Israel linked to a disruptive cyberattack on Iranian port facility - The Washington Post*. https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

Threatpost. (2019, February 5). *The APT Name Game: How Grim Threat Actors Get Goofy Monikers | Threatpost*. https://threatpost.com/the-apt-name-game-how-grim-threat-actors-get-goofy-monikers/141445/

Whyte, C. (2016). Ending cyber coercion: Computer network attack, exploitation and the case of North Korea. *Comparative Strategy*, *35*(2), 93–102. https://doi.org/10.1080/01495933.2016.1176453

Williams, B. T. (2014). The Joint Force Commander's Guide to Cyberspace

Operations. *Joint Forces Quarterly*, *73*(2), 12–19. http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf?ver=2014-04-01-122156-563%5Cnhttp://ndupress.ndu.edu/Media/News/Article/577499/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations/

Wortham, A. (2011). Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force? *Federal Communications Law Journal*, *64*(3), 643–660. http://www.repository.law.indiana.edu/fcljhttp://www.repository.law.indiana.edu/fclj/vol64/iss3/8

Yadav, T., & Rao, A. M. (2015). Technical aspects of cyber kill chain. *Communications in Computer and Information Science*, *536*, 438–452. https://doi.org/10.1007/978-3-319-22915-7_40

ZDNet. (2002, February 19). *Security guru: Let's secure the Net | ZDNet*. https://www.zdnet.com/article/security-guru-lets-secure-the-net/