The International Legal Framework on State-Sponsored Cyber Operations Against International Organizations:

Examining the Russian-Sponsored OPCW Operation and Response

Supervisor: Dr. Shires

Second Reader: Dr. van Steen

Sarah Felicia Estarippa; s2619334

Master Thesis Crisis and Security Management

Leiden University: Faculty of Governance and Global Affairs

June 7th, 2020

Word count: 14.139

Abstract

State-sponsored cyber operations are often below-the-threshold operations and do therefore neither identify as armed attacks, nor fall under the law of self-defense. The lack of international agreement on international law regarding cyber operations results in legal uncertainty. This includes cyber operations against international organizations. The question arises whether hosting states should be held responsible to act upon cyber operations against international organizations. This thesis provides a literature review on the single case study of the cyber operation in April, 2018, against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. The OPCW prevents the production and use of chemical weapons. During the Russian-sponsored operation, four officers from the Russian military-intelligence agency Glavnoje Razvedyvatel'noje Upravlenije (GRU) travelled to The Hague with the equipment to get access to the Wi-Fi network of the OPCW. International law argues that an infringement of sovereignty occurs when an international organization is unable to perform its inherently governmental functions. At the time of the operation, the OPCW was looking into the possible Russian involvement in the poisoning of the double-spy Sergei Skripal and his daughter as well as the chemical attack in Douma, Syria. The Russian-sponsored cyber operation could have interfered with the investigations. This was also the case with the MH17 investigation. Interference with the investigations would have undermined the functioning of the OPCW. Therefore, one could argue that the Russian cyber operation was an infringement of sovereignty of the involved states. The possible intended result of the cyber operation could have affected not only the Netherlands, but all 193 supporting states. In general, the hosting state has the responsibility to respond. In addition, the agreement between the OPCW and the hosting state mentions that the Netherlands is responsible for the safekeeping of its headquarters. Therefore, the Netherlands had arguably the right to respond in accordance with international law. Also, the response itself, to evict the GRU officers as unwanted persons, is a response of retorsion and is in accordance with international law. Whether or not the response was appropriate to prevent similar operations that undermine the rule of law, remains unclear and should be further researched. Gaps in international documents, like the EU Cyber Diplomacy Toolbox, regarding the application of international law to international organizations, remain. This results in the inability to properly govern cyber operations, like the OPCW operation, and to prevent similar cyber operations in the future.

Keywords: Cyber Operations, International Law, International Organization

Table of Content

1. Introduction

1.1 Introduction to Cyber Operations and International Law

The Cyber Operations Tracker (Council of Foreign Relations, 2020) suspects 28 countries of sponsoring cyber operations. Most (known) cyber operations are 'below-the-threshold' operations. These operations are not subject to the law of self-defense because they are not identified as armed attacks (Boeke, Broeders & Georgieva, 2019). Attributing responsibility to a state-sponsored actor who committed the cyber operation is difficult and has technical, political and legal aspects. The source has to be identified and questions arise concerning who should make the attribution to the accused state. When a state is attributed, this could set in motion legal consequences (Eichensehr, 2020).

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt, 2013) is one of the most well-known academic works that examines the applicability of international law to cyber conflict and warfare. The manual focuses on military-dominated laws and regulations that are applicable to cyber-attacks in which force is used. However, the international legal framework is only applicable to cyber warfare and not to all operations in cyberspace. This is because not all cyber operations are disruptive and destructive (Boeke & Broeders, 2018). Therefore, a second version of the Tallinn Manual was published. Whilst still acknowledging the importance of the first version, the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Schmitt, 2017) broadens the scope by including the general principles of international law and legal regimes applicable to cyber operations.

The Tallinn Manual 2.0, Rule 4 states the following: *'A State must not conduct cyber operations that violate the sovereignty of another State'* (Schmitt, 2017, p.5.). The question arises whether a state-sponsored cyber operation violates a state's sovereignty (Moynihan, 2019). The international law rules and principles regarding cyber operations are not clearly defined, which makes it difficult to interpret the application. This could lead to the misinterpretation of the responses of states and even to further escalation. States have increasingly sanctioned the "attackers" and state-sponsors (Lotrionte, 2018). For example, economic sanctions were imposed against North Korea by the United States (US) in response to the Sony Pictures Entertainment cyberattack in 2014. This cyberattack aimed to stop the release of the film *The Interview* and create a negative financial impact on the company which would restrict the freedom of expression (Roberts, 2015). Still, sanctioning appears

insufficient since cyber operations continue to be committed by (non-)state actors (Lotrionte, 2018).

1.2 Research Questions

The legality of intelligence gathering is contested in international law. To what extent it is proportionate remains vague (Forcese, 2016). Some argue that peacetime espionage is covered by international law and is an illegal act due to its intrusive nature and because it violates a state's sovereignty (Buchan & Navarette, 2019). However, the legality of cyber espionage remains contested. It is dependent on the way through which it is carried out. This is further discussed in section 5.1.1. In addition, when cyber operations are conducted by foreign intelligence agencies, the legality remains unclear (Boeke, Broeders & Georgieva, 2019).

The cyber operation against the Organisation for the Prohibition of Chemical Weapons (OPCW), which was carried out by the Russian military-intelligence agency Glavnoje Razvedyvatel'noje Upravlenije (GRU), aimed, possibly, to influence investigations. The operators were physically present at the territory of the operation in the Netherlands. This enables the correct attribution to a state. The GRU officers travelled to the Netherlands, the Hague, to hack into the Wi-Fi network of the OPCW (BBC, 2018). The OPCW was looking into two cases in which Russia was accused of being involved. It is a possibility that the GRU attempted to compromise the investigations of the OPCW (Sander-Zakre, 2018). However, they were stopped by the Dutch Military Intelligence and Security Service (MIVD) before the GRU officers were able to get access to the OPCW network (Wintour & McKernan, 2020). The Dutch Minister of Defense, Ank Bijleveld, declared that this was a wrongful act according to international law without further explanation (Government of the Netherlands, 2018). She even stated that that the Netherlands is in a state of "cyberwar" with Russia (Moes, 2019). In addition, in a letter to the Dutch House of Representatives (Bijleveld, 2018), she stated that 'undermining the integrity of international organizations, is unacceptable.' (p.4.).

This thesis aims to investigate the appropriateness of these claims and pinpoint to what extent cyber operations against international organizations are in fact undermining the international rule of law. In addition, it is examined whether or not it was appropriate of the Dutch Minister of Defense to respond on behalf of an international organization. Therefore, the aim is to answer the following research question:

To what extent do state-sponsored cyber operations against international organizations violate international law?

To answer this research question, the case of the OPCW will be researched in-depth, with the purpose of answering the two following research questions:

(1) To what extent was the intended cyber operation against the OPCW in violation with international law?

(2) To what extent is the response of the Netherlands to the OPCW cyber operation appropriate, in accordance with international law?

The first question looks at the legality of the operation carried out by the Russian military-intelligence agency GRU. The second question looks at whether or not the response of the Netherlands was appropriate considering that the operation was aimed at an international organization.

1.3 Academic and Social Relevance

The following section explains the academic and social relevance of investigating this topic. First, the academic relevance is discussed. Academic relevance looks at the extent to which this thesis benefits and fills in knowledge gaps in the multidisciplinary field of cybersecurity. After, the social relevance is examined which concerns the contribution to society at large.

1.3.1 Academic Relevance

There is a lack of scholarly work on the application of international law on cyber operations. It is important to understand cybersecurity not only as a technological issue, but also as an issue regarding applicability of laws and regulations. The emergence of cyberspace is accompanied by grey zones in domestic and international law (Moynihan, 2019). The Tallinn Manual (as discussed in section 1.1) is the most comprehensive work on cyberspace and international law but lacks states' participation and is non-binding (Adams & Reiss, 2018).

The main focus in scholarly work lies on the applicability of the law of war to cyber operations. However, the military legal framework does not suit best in application to cyberspace (Boeke & Broeders, 2018). Furthermore, scholarly work does not cover the application of international law to international organizations and in cyberspace. Liis Vihul,

the Chief Executive Officer of Cyber Law International, stated that it should be determined whether the application of international law in cyberspace is sufficient. In particular, to what extent cyber operations against international organizations should be prohibited. Vihul mentioned that the OPCW operation should be taken as an example upon which this claim could be examined (United Nations, 2018).

1.3.2 Social Relevance

It is also socially relevant to research the topic since cybersecurity plays a growing role in today's world politics. Information in cyberspace can attract citizens with a certain ideology, also defined as soft power. Cyberspace can also be used as hard power in which damage is done to physical targets. An important example of hard power in cyberspace is the cyberattack against the Iranian nuclear facility in 2010. A malicious computer worm, Stuxnet, was used to target the Supervisory Control And Data Acquisition (SCADA). This disrupted approximately 1,000 centrifuges which are assumed to have slowed down the nuclear program of Iran. Therefore, Stuxnet is also considered to be the first known weapon used in cyberspace (Nye, 2011).

Cybersecurity also concerns national security and public safety, upon which cyber operations can have destructible consequences (Tsakanyan, 2017). Cyber operations can, for example, harm infrastructure which could affect the conduct of essential services (Gisel & Olejnik, 2018). Still, the application of international law in cyberspace remain ambiguous and contested. Liis Vihul (United Nations, 2018) argued that states have the right to respond and apply countermeasures to situations that are unlawful. The response can either serve as a warning to stop further malicious cyber activities or as a start of ongoing cyber operations (also known as a "cyberwar") (van der Meer, 2018). To ensure the governance of cyber operations and prevent hostile operations from occurring in the future, it is of great importance to cover this topic. This enables clarity on the application of international law to these cyber operations.

1.4 Thesis Structure

In order to answer the research questions, this thesis is divided into different sections. First, a theoretical framework is presented to establish the positioning within the relevant body of knowledge. Second, the research design and methods section examines how and what data is going to be collected. Third, the case of the OPCW cyber operation is explained as

well as the responses to this operation. After, an overview is provided regarding the international laws and regulations at stake. Furthermore, the analysis section applies the international law to the case. Last, the conclusion and discussion sections are provided. The conclusion answers the research questions, as set out in section 1.2. The discussion section gives the limitations, implications and suggestions for future research.

2. Theoretical Framework

The theoretical framework provides a positioning in the body of knowledge and conceptualizes terms used in the research question. This is done to prevent misunderstandings and to provide a clear overview of what is being researched. First, the broader field this thesis looks at is discussed which holds the concepts of cyberspace and cybersecurity. After, the definition and examples of cyber operations are provided to ensure a clear understanding of the kind of cyber operations that can occur and are examined. Followed by the last section in which international law in relation to cybersecurity examines how laws and regulations are applicable and where potential gaps lie.

2.1 Cyberspace and Cybersecurity

The law of war regulates different domains in which warfare can be conducted. The four classic domains of warfare are land, sea, air and space (Schmitt, 2013). In 2016, cyberspace was recognized as the fifth domain of warfare at the North Atlantic Treaty Organization (NATO) Warsaw summit. Still, no definition can be found in the document or on their website. Since the mid-90s, the concept of cyberspace has been discussed and contested and there is still no single definition (Kamer, Starr & Wentz, 2009). This could be due to the fact that cyber(space) continuously evolves. The Department of Defense (DoD) also declared cyber as a domain in the information environment. Since this thesis does not examine cyberattacks which could fall under the law of war, but rather cyber operations, this definition is important. The definition of cyberspace as provided by DoD (2020) is:

> *'Cyberspace is a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.'* (p.55.).

For cybersecurity, unsurprisingly, a consensus on a definition is still absent as well. It varies across nation-states, academics, organizations, governments and the private sector. Some focus more on the technical side and others on the security side of cybersecurity (Kremling & Parker, 2017). Since this thesis focusses on the case of OPCW in which Russian intelligence officers travelled to the Netherlands, the definitions of cybersecurity from the Netherlands and Russia are provided. The Dutch definition can be found in the National Cyber Security Strategy 2:

'Cyber security refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred. Such damage may consist of any or all of the following: reduced reliability of ICT, limited availability and violation of the confidentiality and/or integrity of information stored in the ICT systems.' (Opstelten, 2014, p.7.).

This definition focusses rather on the security aspect and the Cyber Security Strategy mainly discusses the threats that need to be prevented in Information and Communication Technology (ICT) (Opstelten, 2014). The definition of the Russian government of "cybersecurity", according to the National Security Concept of the Russian Federation, is:

'a set of conditions under which all components of cyberspace are protected from the greatest possible number of threats and influences with undesirable consequences. Cyberspace is a field of activity in the information space, formed by a combination of communication channels of the Internet and other telecommunication networks, the technological infrastructure that ensures their functioning, and any forms of human activity carried out through their use (person, organization, state).' (Cooperative Cyber Defense Centre of Excellence, 2000, p.2.).

It should be noted that Russian documents talk about information security rather than cybersecurity. Information security encompasses safekeeping of individuals', organizations' and states' interest from negative impact regarding information (Cooperative Cyber Defense Centre of Excellence, 2000). This is an important distinction to keep in mind since this thesis discusses cyber operations that manipulate data. Cybersecurity concerns the security in cyberspace either regarding information or other things. Information security, on the other hand, concerns the security of information regardless in which "space" (either cyber or analog) this is (Irwin, 2018).

As mentioned in section 1.1, state operations in cyberspace do not always fall under the laws of warfare. The notion that Russia refers to information security rather than cybersecurity also leads to the question whether information warfare should be applicable. Information is considered to be an important asset as it enables to control (amongst others) over economic productive capacity and military forces. The ability to manipulate information has therefore become securitized (Collins, 2016). The different view of information security, will be further discussed in section 7.2.3.

2.2 Cyber Operations

A cyber operation is defined by the US Department of Defense (DoD) (2020) as:

'The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Also called CO.' (p.56.).

There are different activities that occur in cyberspace to achieve an objective and that are important to cybersecurity. These different activities encompassing cyber operations include: Distributed Denial of Service (DDoS), espionage, defacement, data destruction, sabotage, doxing and data manipulation (Council on Foreign Relations, 2020). Data manipulation is the focus of this thesis which refers to the process of changing or deleting data for a particular gain. The tools used for a cyber operation are called "malware", a word-combination of "malicious" and "software" (Modderkolk, 2019). Different actors are able to perform cyber operations; individuals can act alone or in a hacking group. This makes it difficult to prevent certain cyber operations from disrupting systems or to attribute the correct actor to the operation (Granova & Slaviero, 2017). The cyber operation examined in this thesis is the attempted data manipulation by Russian intelligence officers at the OPCW, which will be further discussed in Chapter 4.

2.3 International Law regarding Cybersecurity

After the Cold War, states and other actors have increasingly been critical of international law. More states are using force outside of what would be in accordance with the United Nations (UN) Charter (Delerue, 2019). In addition, the emergence of cyberspace is accompanied by new obstacles and challenges. One of the main challenges lies in the fact that the perpetrator's identity often remains unknown. If the operation takes place from outside the targeted nation, international collaboration is often required which could lead to further barriers (Moynihan, 2019). Still there are several obligations in cyberspace in accordance with international law. For example, the 2013 and 2015 reports of the UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, recognize that the UN Charter and international law are applicable to cyberspace (Delerue, 2019).

The Dutch legal positions assign the following obligations in cyberspace to states: sovereignty, non-intervention, the prohibition on the threat or use of force, due diligence, International Humanitarian Law (IHL) and International Human Rights Law (IHRL) (Schmitt,

2019). In addition, states have the right to respond to unlawful acts through countermeasures. These, for example, hold denying aircrafts to land or impose financial sanctions (United Nations, 2018). Other possible response options are: retorsion, necessity and self-defense (Schmitt, 2019). These relevant international obligations and response options will be further discussed in Chapter 5. The emphasis of this thesis lies on the aspect that the Dutch Minister of Defense responded to a cyber operation conducted not against a Dutch organization, but an international organization which is supported by 193 states (Ministerie van Defensie, 2018). The question arises whether or not this was in accordance with international law. The following section will first explain in more detail why the OPCW case was chosen for this thesis.

3. Research Design & Methods

The research design looks at what a single case study is and why it is a good fit for this particular thesis. The research methods explain how empirical data is collected, processed, and analysed. Last, the limitations to answering the research question in a reliable and valid way are discussed.

3.1 Research Design

This section explains what a single case study entails and why it was chosen for this thesis. This includes indicating the pros and cons. After, several cases that are related to the topic will be explained to ensure a proper understanding of the knowledge provided by other cases, which leads to the case selection of the Organisation for the Prohibition of Chemical Weapons (OPCW) case.

3.1.1 Single Case Study

Even though there is no consensus on how to define a case study, Robson (1993) gives the following definition:

> *'A strategy for doing research which involves an empirical investigation of a particular contemporary phenomenon within its real-life context using multiple sources of evidence.'* (p.146.).

Single case study research is conducted when there is a lack of understanding of a certain phenomenon. It is not possible to base generalizations on; it is therefore used to create the first building blocks to propose new research or future continuation. The case is either critical, which holds it is a specific case, or unique, which means it is a rare phenomenon (Yin, 2018). For this study, single case study research is appropriate since no building blocks yet exist that examine the applicability of international law to state-sponsored cyber operations against international organizations; focussing on both the act and the state response. Often it is difficult to attribute the actor since operations can be conducted without being able to trace the operator. The OPCW case (which is explained in detail in Chapter 4) is a specific and critical case since it enables the correct attribution to a state because the Russian GRU officers were physically present at the place of the operation (Mebius, 2018). In short, this thesis aims to provide an in-depth analysis to create the first building blocks of the application of international law and cyber operations that are conducted against an international organization.

3.1.2 Case Selection

The three important components of the research questions (as imposed in section 1.2) that this thesis looks at are (1) state-sponsored (in particular the Russian intelligence agency GRU) cyber operations against (2) international organizations with the (3) involvement of the Netherlands. A selection of some well-known cases can be divided into different categories as shown in the following diagram:

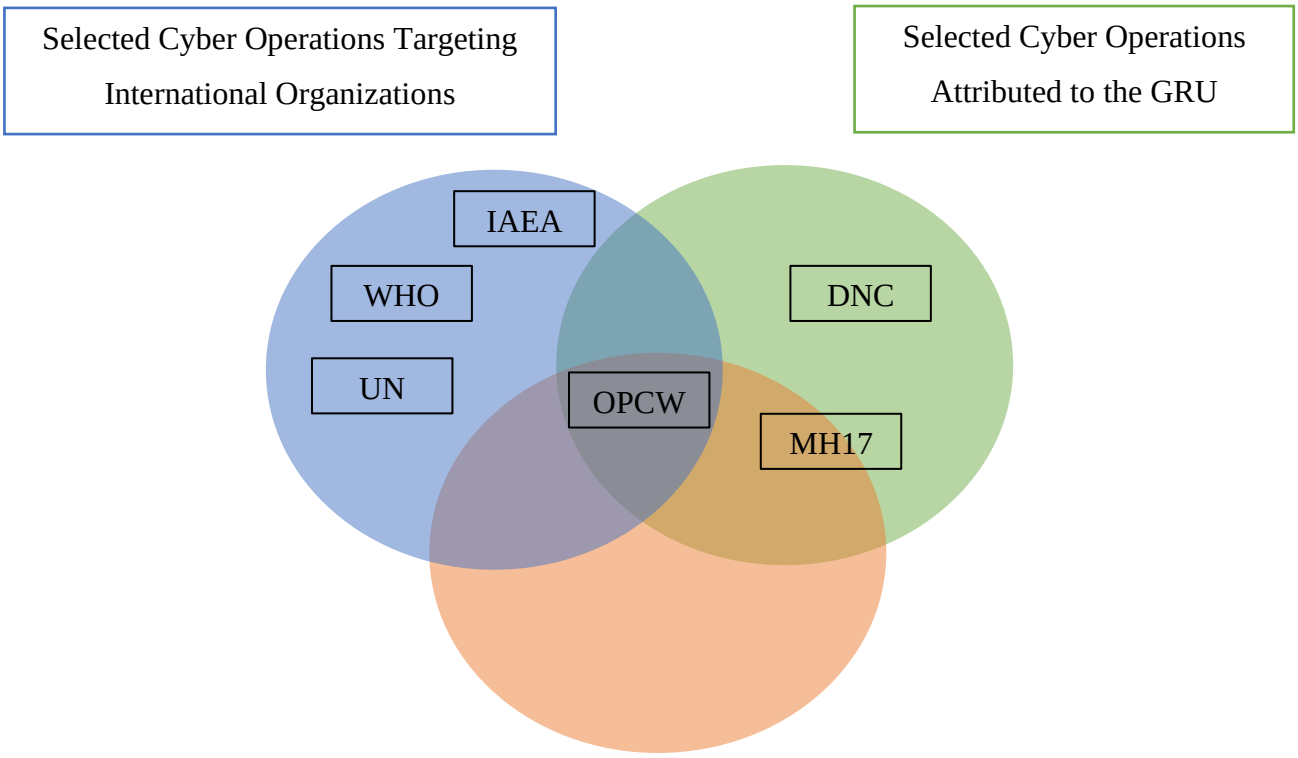

Diagram 1

Case Selection Overview

It should be noted that not all cyber operations that occur are known. Therefore, the following examples do not necessarily encompass all or most important cases. These cases are analysed on the kind of operations as well as the intent, the response, and the applicability of international law. They are examined per category in chronological order.

3.1.2.A Selected Cyber Operations Targeting International Organizations

The first category concerns the involvement of an international organization to examine how the hosting states responded. In the first case, the International Atomic Energy Agency (IAEA), an international organization located in Vienna, Austria, faced a cyber threat in 2007. The cyber operation against the IAEA concerned an Iranian hacker who aimed to get access to information regarding Iran's atomic activities. However, the head of the IAEA, Yukiya Amano, claims no information was stolen (Reuters, 2012). Another cyber operation against the IAEA concerns the hacker group Anonymous. They claimed to have sensitive information which they threatened to publish if the IAEA would not investigate the nuclear program of Israel. After the second operation, Mr. Amano did recognize that information of IAEA scientists was hacked but added that it did not concern sensitive information on Iranian atomic activities (Kelley, 2012). Both operations were anti-Israel. However, since the IAEA is located in Austria it is of importance to examine if and how Austria responded. A response appears to be non-existent. In neither cases prosecutions were conducted.

The second international organization, the offices of the United Nations (UN) in Vienna and Geneva, faced a hack in July, 2019, in which 42 core servers were affected. This includes password management and security firewalls. The report on the hack did not appoint a specific state or group to the case (VOANews, 2020). The offices in Geneva and Vienna decided not to make the breach public and no responses were present from the hosting nation-states of the offices. It might be questioned whether the UN adhered to the General Data Protection Regulation (GDPR). However, due to its diplomatic status this is not an obligation for the UN and can therefore not be held accountable (Winder, 2020).

The third and most recent case concerns the World Health Organization (WHO) which was a victim of hackers this year (2020) during the coronavirus pandemic. It is not known who the hackers are but on March 13th, a malicious website was discovered which imitated the WHO's email system. The motives behind the cyber operation are still unclear. In addition, besides an alert posted by the WHO, no other responses were (as of today) given (Satter, Stubbs & Bing, 2020).

3.1.2.B Selected Cyber Operations Attributed to the GRU

The second category considers the involvement of the GRU in cyber operations. One of the cases in which the involvement of the GRU was apparent, was the hack of the governing body for the United States Democratic Party, the Democratic National Committee (DNC). In 2015 and 2016, hackers gained access to the computer network of DNC which was

attributed with high confidence to the Russian intelligence agency GRU. These attacks were meddling with the American election in 2016, however, there is no evidence that the outcomes were affected by this. In addition, other attacks against the DNC resulted in thousands of emails and passwords being stolen and posted on websites such as DCLeaks.com. Therefore, the United States charged twelve GRU hackers who registered this website (Ng, 2018). In addition, the United Kingdom attributed the attacks to the GRU and stated that they undermined international law as they do not have a national security interest (Muncaster, 2020).

3.1.2.C Select Cyber Operations Involving the Netherlands

The MH17 investigation was victim of a cyber operation and concerns both aspects of the GRU and Dutch involvement. On July 17th, 2014, the MH17 Malaysia Airlines flight was shot down. The Joint Investigation Team (JIT), a combination of authorities from the Netherlands, Belgium, Malaysia, Ukraine and Australia, investigated the case between 2015 and 2017. The investigation faced a cyber operation conducted by GRU. It is important to note that this section is not regarding the MH17 case itself but the investigation on the MH17. A laptop from the GRU contained evidence that the investigation's database was intercepted (Goud, 2020). Russian officers were prosecuted for shooting down the MH17 case itself. However, no prosecutions were held regarding the attempt to hack the investigation (Openbaar Ministerie, 2020).

3.1.2.D Thesis Case Selection

As can be seen in Diagram 1, this thesis focusses on the cyber operation against an international organization located in the Netherlands and involving the GRU. This is the OPCW cyber operation case which is further discussed in Chapter 4 after the research methods and limitations are explained. An important detail why the OPCW case is a good selection is because the MIVD was involved (Ministerie van Defensie, 2018). Therefore, the Netherlands as a state was able to respond besides the response of the international organization itself. This distinguishes this particular case from others in this category. In addition, the examples of cases provided in the previous section show that little to no response was conducted by hosting states or states involved. The responses mainly comprised of attribution of the cyber operation to an actor. Therefore, the OPCW case is chosen as it enables the examination of the appropriateness of the response by the hosting state.

3.2 Research Methods

The research methods explains how and which empirical data is going to be collected. It is important to have different data sources to create a thick description of the case at hand and to enable a full understanding from different points of view. The research methods first explain how data is collected. Data resources have to be analysed on feasibility, validity and reliability. Secondly, this section describes how the data is analysed.

3.2.1 Data Collection

Data collection consists of reports and other documents accessed through on- and offline sources, for example Google, Leiden Library, and Google Scholar. These documents consist of primary sources such as the NATO's summit on international law and cyberspace (North Atlantic Treaty Organization, 2016), the Dutch international cybersecurity strategy report (Government of the Netherlands, 2017), and the evaluation report of the cyber operation (e.g. Nationaal Cyber Security Centrum, 2013; National Coordinator for Security and Counterterrorism, 2019). In addition, as was stated in Minister of Defense Ank Bijleveld's letter, the Ministerie van Defensie (2018), Algemene Inlichtingen- en Veiligheidsdienst (2018) and Cybersescuritybeeld Nederland year reports of 2018 describe and analyse the security threat the GRU poses to the international rule of law. Furthermore, the Nederlandse Cyber Security Agenda (Rijksoverheid, 2018) and the Geïntegreerde Buitenland- en Veiligheidsstrategie (Rijksoverheid, 2018) set out that cyber threats will be answered on a national and international level. Also, statements are examined (e.g. OPCW, 2018) as well as secondary sources like news reports, for example the Guardian (Crerar, Henley & Wintour, 2018) and DutchReview (van Leeuwen, 2018). Last, scholarly work will be assessed through Google Scholar and Leiden Library using the search terms: 'International', 'Law', 'Cybersecurity', also in combination with 'OPCW', 'Response', 'Cyber' and/or 'Operation'. Results will be selected based on relevance by reading the title and abstract. Other examples are the Tallinn Manual 2.0 (Schmitt, 2017), part of Delerue's (2020) book and article (2019) on *Cyber Operations and International Law* and the EU Cyber Diplomacy Toolbox (Moret & Pawlak, 2017).

3.2.2 Data Analysis

The document analysis examines the data collected as described in the previous section. The general rule of law and the application of the OPCW case will be discussed. Furthermore, suggestions will be made regarding possible intervening causes and changes in policies and/or the rule of international law regarding cyber operations with similar modus

operandi and similar motives to the GRU cyber operation against the OPCW (e.g. see The United States Department of Justice, 2018).

3.3 Limitations: Reliability and Validity

There are limitations to the reliability and validity of this research which are important to keep in mind. Reliability refers to '*the extent to which scores from a measure are free from random error.*' (Maruyama & Ryan, 2014, p.192.). Validity concerns '*the extent to which scores reflect only the desired construct without contamination from other systematically varying constructs.*' (Maruyama & Ryan, 2014, p.192.). This section examines both limitations to answering the research questions as imposed in section 1.2.

3.3.1 Limitation: Reliability

A limitation to reliability relates to the fact that data on cyber operations are not always available since nations usually keep this information private. When nations are aware of other nations trying to infiltrate the system, deterrence is often not the first response. This information is kept under the radar to prevent the opponent from knowing another state's position. In other words, it is not clear what everyone knows or is capable of doing in the field of cybersecurity. Furthermore, international law is often ambiguous and leads to different interpretations. With the evolving cyber capabilities, there is not one definition for cyberspace or cybersecurity (as discussed in section 2.1). Whether or not international law is applicable and to what extent international law has been violated, is difficult to examine. In addition, this thesis focusses on intended data manipulation operations. The OPCW operation was stopped before data got manipulated, according to the MIVD. This makes it more difficult to apply international law as the focus lies on the intent of the operation. The intent is further discussed in section 6.1.1.

3.3.2 Limitation: Validity

The validity is limited because it is difficult to show the direct relation between international law and the cybersecurity responses. One should take into account the pre-political relations between the Netherlands and Russia. For example, regarding MH17 and the attempted murder of the defected Russian spy Sergei Skripal (these cases will be explained in detail in section 4.1). These also could have led to the Dutch Minister of Defense declaring a "cyberwar". Since this thesis provides one case study regarding international law in cyberspace, future research could apply international law to other (similar) cyber operation

cases to examine whether or not significant errors and gaps exist in international law to create classifications and implications in order to have a wider impact. In addition, future research should continue to address the question whether a hosting state is responsible to act when an international organization is the target of a cyber operation. This is further discussed in section 7.2.3.

4. Case Description

The following section explains the cyber operation against the Organisation for the Prohibition of Chemical Weapons (OPCW) conducted on the 13th of April, 2018. This includes looking at possible reasons why the OPCW was of interest to Glavnoje Razvedyvatel'noje Upravlenije (GRU). After, the response to this operation by the Netherlands will be discussed to ensure a proper understanding of the case at hand. The last section explains why the GRU was already on the radar of the MIVD which enabled them to stop the cyber operation in time.

4.1 OPCW Case

To explain the case of the OPCW, background information will first be presented to gain a better understanding of the issues at stake before the alleged operation occurred. After, the case will be explained in detail. Last, it is explained how the GRU was stopped on time by the MIVD.

4.1.1 Background

In April 2018, the OPCW was conducting research regarding the poisoning of a former Russian double spy Sergei Skripal and his daughter Yulia Skripal on March 4th. Sergei Skripal worked for the GRU and as a double agent for the UK's Secret Intelligence Service. He settled in the UK after being accused of high treason by the Russian court. Two Russians, Alexander Petrov and Ruslan Boshirov, travelled to the UK and were suspected of using a military-grade Novichok nerve agent (BBC, 2018). This nerve agent disables the normal functioning of the nervous system and can therefore lead to fatality (Therrien & Roxby, 2018). Sergei and Yulia Skripal were found unconscious in Wiltshire but survived.

Furthermore, the OPCW was looking into the case of the chemical attack on the Syrian city Douma by Bashar al-Assad, an ally of Russia in the Syrian conflict. On April 7th, Douma was attacked and approximately 40 to 50 people died and 100 were injured. Due to the Russian history with chemical weapons and previous threats towards Syria, Russia's involvement was investigated (Wintour & McKernan, 2020). However, Russia accuses the UK of staging the attack by faking pictures of victims, supposedly taken before Russia arrived in Douma. Russia did not provide evidence to prove that it was a set up (CBSNews, 2018). Both cases are of great importance to Russia due to its suspected involvement. They could

therefore be argued to play a role in the alleged interference of the GRU at the OPCW (Mebius, 2018).

4.1.2 The OPCW Case

On April 10th, 2018, four officers of the Russian military intelligence agency GRU travelled from Moscow to Amsterdam Schiphol Airport with diplomatic passports. Aleksei Morenets, Evgenii Serebriakov, Oleg Sotnikov and Alexey Minin conducted a cyber operation against the Organisation for the Prohibition of Chemical Weapons (OPCW). They rented a Citroën C3 to travel to the OPCW. In the car, they placed a laptop and hacking devices, covering the Wi-Fi panel antenna with a coat. They also brought 20.000 euros and 20.000 dollars in cash. Concluding from the devices present, they aimed to commit a close access-hack operation to get into the OPCW's Wi-Fi-network. What the goal of the operation was, remains unclear. On April 13th, the Russian officers travelled by car to the closest hotel near the OPCW, which is the Hague Marriott Hotel, whilst being watched by the Dutch Military Intelligence and Secret Service (MIVD). When the devices in the Citroën were signalled as active, the MIVD set in motion a disruptive operation.

The attempted cyber operation was stopped. However, the MIVD is unsure whether or not information was gathered by the Russian officers. The MIVD captured the car as well as their phones. The Russians intelligence officers threw their phones on the ground in attempt to break them, but their attempt was unsuccessful. The phones proved that the Russians were from the GRU: one phone was connected to a gsm-mast closest to GRU operating location. Serebriakov's search history on his laptop showed that searches were conducted to investigate the Hague Marriott Hotel and the OPCW (Mebius, 2018). The Russian officers were escorted to the airport and had to leave the country as unwanted persons. It could be argued that they attempted to compromise the two investigations that were important to Russia (Sanders-Zakre, 2018). The intent of the Russian cyber operation is further discussed in section 6.1.1.

4.1.3 The GRU on the Radar of the MIVD

Russia was already on the radar of the MIVD after the Malaysia Airlines Flight (MH17) incident (as discussed in section 3.3.1). On July 17th, 2014, the flight from Amsterdam to Kuala Lumpur was shot down. All 298 people on board, including crew members, died. The Dutch Safety Board (OVV) investigated the incident, besides the Joint Investigation Team (JIT), and concluded that the airplane was shot down by an only in Russia manufactured Buk missile. The OVV investigation looked into the flight route determination decision-making process, whilst the JIT conducted the criminal investigation (Weaver, 2015).

The reports of the Algemene Inlichtingen- en Veiligheidsdienst (AIVD) (2018) and National Coordinator for Security and Counterterrorism (2019) state that Russia has an offensive cyber programme aimed to disrupt and sabotage vital Dutch infrastructures. The Dutch Minister of Defense was already informed of the Russian Federation's interest in the investigation on MH17. After follow-up research it became clear that the GRU was manipulating and influencing research on MH17 in Malaysia. The Netherlands took measures to point out the digital threats caused by Russia and therefore the GRU was already on the radar before they targeted the OPCW (Ministerie van Defensie, 2018).

4.2 Response of the Netherlands to the OPCW case

As mentioned in section 4.2.2, the Russian GRU officers present at the OPCW case were escorted to the airport and evicted as unwanted persons. The Dutch Minister of Defense, Ank Bijleveld, wrote a letter to the Dutch House of Representatives to explain the disruption of the GRU cyber operation. This is not the first cyber operation committed against an organization. As stated earlier and mentioned in section 3.1.1, the GRU has operated against the investigation of MH17. Furthermore, the Dutch Minister of Defense argued that a response by the Netherlands was appropriate since it is the host-country of the international institute which prevents the use of chemical weapons and to ensures its safekeeping (Ministerie van Defensie, 2018).

The UK confirmed the Dutch allegations against the Russian officers and supported the Netherlands stating that these cyber operations conducted by the GRU undermine the international legal order. British officials refused to answer the question if they would have taken the same actions if the incident would have been in the UK. They did stress that the operational decisions were rightfully determined by the Dutch authorities (Crerar, Henley & Wintour, 2018). In addition, the US publicly holds charges against GRU officers and asked for support from the Dutch Public Prosecutor's office, to which the Netherlands Defense Intelligence and Secret Service (DISS) launched its own investigation. NATO Allies support the responses of the Netherlands and the UK to publicly call out the operation and demand Russia to stop this type of behaviour (North Atlantic Treaty Organization, 2018). The Dutch Minister of Defense continued that these exposures are to warn the Russian Federation that these activities are unacceptable (Ministerie van Defensie, 2018).

5. International Law

Cyberspace is seen as the fifth domain in which international law applies (as mentioned in section 2.1). However, the applicability itself remains vague and contested. It is essential to create clarity on the application of international law in cyberspace (Government of the Netherlands, 2019). Therefore, this section will start with an overview of the most relevant international laws regarding international organizations, cyber operations and state responsibility (to respond). First, the focus is on state-sponsored cyber operations against international organizations. After, the responsibility to respond to cyber operations is examined. The main source used in this chapter is the Tallinn Manual 2.0, part of Delerue's book on cyber operations and international law, as well as the EU Cyber Diplomacy Toolbox (as mentioned in section 3.2.1). It should also be noted that positions regarding international law and cyberspace differ per country; therefore, this thesis also considers the position of the Netherlands in particular to examine the appropriateness of the response from its point of view.

5.1 State-sponsored Cyber Operations against International Organizations

The first research question of this thesis focusses on the legality of state-sponsored cyber operations against international organizations. To examine this, first the legality of different cyber operations is looked at including the legality of state-sponsored operations. After, sovereignty and infringement are analysed regarding international law. Finally, it is important to discuss the applicability of international law to international organizations considering that the Organisation for the Prohibition of Chemical Weapons (OPCW) is an international organization and therefore does not fall under one state's authority.

5.1.1 Cyber Operations

The focus of this thesis lies on cyber operations and not on "cyber-attacks". The word attack invokes the use of the law of armed conflict. However, most cyber operations do not leave physical evidence and in most operations, force is not used (Moynihan, 2019). Therefore, this section will not look at international laws and regulations regarding the use of force or armed conflict but those operations which fall outside this scope. It must first be noted that not all cyber operations are regulated by international law (Schmitt, 2017). There is only one kind of cyber operation discussed in the Tallinn Manual 2.0 which does not identify as a cyber-attack: peacetime cyber espionage. However, this is not the only cyber operation conducted that is not identified as a cyber-attack. Cyber espionage is:

'any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information.' (Schmitt, 2017, p.168.).

This rule solely applies to state-sponsored cyber espionage. As stated in the Tallinn Manual 2.0 (Schmitt, 2017), Rule 32, this kind of cyber operation is not per se in violation with international law; it depends on the method through which it is carried out. This is closely related to the principle of sovereignty (as discussed in the following section) and prohibition of intervention (see section 5.2.1). In addition, some cyber operations could enable cyber espionage but are not espionage operations per se. These cyber operations must be assessed on legality on its own (Schmitt, 2017).

Cyber espionage is not the only type of cyber operation conducted in cyberspace. However, no legal definitions exist for, for example, information (often referred to as data) deletion or manipulation. In general, data manipulation in cybersecurity holds that data is slightly tweaked for a particular gain (Nettles, Merulla & Warzala, 2019). In general, the focus does not lie on the cyber operation itself, but rather on the (possible harmful) effect. The Tallinn Manual 2.0 (2017) describes that cyber operations can cause damage or destruction, either physical or non-physical (e.g. destroying data from a hard drive). The destruction could belong to a natural or legal person. Therefore, data destruction can be considered to violate Article 17 of the Universal Declaration of Human Rights (UDHR) which concerns the right to own property. In addition, it could also be seen as a violation of the right to privacy. Especially when it concerns sensitive information in, for example, investigations conducted against state actors.

As mentioned by Boeke, Broeders & Georgieva (2019), it should be clear that covert cyber operations should have oversight and be examined on proportionality and necessity. In general, cyber operations are not unlawful per se, however, they can be when their effect violates international law. Therefore, the question also arises whether the intent to conduct a cyber operation is in violation with international law when it could have an illegal effect. This increases the debate on cyber operations and their legality and is particularly of interest to the OPCW case since there was no physical effect. This will be further discussed in section 6.1.1.

5.1.2 Sovereignty and Attribution

The rule of sovereignty holds that states are independent and is also applicable in cyberspace (Schmitt, 2017). It implies that states have jurisdiction over their territory within the boundaries of international law. Furthermore, sovereignty implies that states are free to

determine their own obligations as long as they respect international law. Still, states have the obligation to respect other states' sovereignty (Government of the Netherlands, 2019). There are no arguments that this principle does or should not apply in cyberspace (Moynihan, 2019). However, the limits of territory are less clear in cyberspace. Cyber operations can involve cross-border components and therefore potentially infringe a state's sovereignty. What these cyber operations entail, is still contested (Government of the Netherlands, 2019). Rule 4 of the Tallinn Manual 2.0 (Schmitt, 2017), as mentioned in section 1.1, states that the infringement of sovereignty occurs when a state's territorial integrity is targeted and when there has been an interference with inherently governmental functions of another state. Though there is no consensus on the definition of "inherent governmental functions", deleting data is included in this rule of infringing a state's sovereignty. In addition, the governmental function does not necessarily have to be conducted by a state but can also be conducted by a non-governmental organization. In general, to be considered as violating a state's governmental functions, the state should also be the target of the cyber operation. The question arises whether or not international organizations such as the OPCW fall under the scope of a state's governmental function. This will be further analysed in the following chapter on the analysis of the OPCW case with regard to the application of international law.

Rule 14 of the Tallinn Manual 2.0 on internationally wrongful acts states that a state can be held responsible for cyber activities when it is a breach of an international obligation (Schmitt, 2017). A state's responsibility for a cyber operation means, according to international law, that the state can be attributed to the operation. There are three different kinds of attribution: legal, political and technical. Legal attribution holds that the victim states attributes the act to a specific state with the aim of legal consequences as there has been a violation of international law. Political attribution, on the other hand, occurs when a policy consideration attributes (for example publicly) a state. Last, technical attribution means that the factual investigation identifies the actor as responsible and therefore holds the right to attribute. Evidence is not a necessity to attribute a state to a cyber operation. This only becomes necessary when legal proceedings are set in place (Government of the Netherlands, 2019). Still, a reliable attribution of a cyber operation to a state remains challenging, especially when trying to enforce cyber sanctions. A wrongful attribution to a state could in turn be in violation with international law. The EU Cyber Diplomacy Toolbox therefore argues that the attribution is a sovereign political decision of individual states but added that

the ability to correct attribution should be improved. In order to establish this, technical research should be conducted (Moret & Pawlak, 2017).

A question which arises is whether a state's sovereignty is violated when another state agent enters the territory of the state without permission. Or whether harmful acts have to be committed first and if so, what qualifies as harmful acts (Moynihan, 2019). Though the physical presence of a state is most of the times not applicable, for this thesis it is important to take into consideration that officers of the GRU were present at the headquarters of the targeted organization of the cyber operation. This will be further discussed in the next chapter.

5.1.3 International Organizations

International organizations do not fall under the scope of international conventions. This is due to the fact that international organizations are not recognized as having their own identity and personality. However, this does not necessarily imply that they do not have to adhere to international law (Klabbers, 2017). The International Law Commission (United Nations, 2011) mentioned that responsibility of international organizations with regard to international law remains vague and unclear because there are many different types of international organizations with different functions.

Regarding the attribution of an international organization to the state, Article 4 (1) of the International Law Commission (ILC) states:

'The conduct of an organ shall be considered an act of that state under international law whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the state..(...).'

In addition, the rules regarding the relation between the international organization and the hosting state is set down in an agreement. The hosting state usually holds responsibility for proper functioning of the international organization (Barros, Ryngaert & Wouters, 2016). Furthermore, when looking at Article 4(1) of the ILC and the international organization the UN, for example, it is stated that the hosting state could be held internationally responsible for wrongful acts conducted by the international organization. This could also imply that there is some degree of responsibility of the hosting state to be responsible for the international organ present in its territory. However, this is mainly regarding the facilitation of unlawful acts. It should be noted that the agreement between the UN and the hosting country does not have provisions on liability (Gaja, 2006).

The responsibility for an international organization remains contested (this will be further discussed in the following section). As mentioned in section 5.1.1 the legality of the cyber operation is mainly assessed through the effect it has and the responsibility of the state depends on whether or not this effect infringes upon a state's inherent governmental functions (as mentioned in section 5.1.2). Finally, it is important to keep in mind that the hosting state holds a degree of responsibility to ensure that an international organization can function properly. This will be further analysed to the OPCW case in Chapter 6.

5.2 Responsibility of Responding to Cyber Operations

The second research question looks at the responsibility of a state to respond to cyber operations against international organizations considering that these international organizations do not belong to one state. This was to some degree discussed in the previous section. Still, the question arises whether the hosting state of an international organization holds the responsibility of responding to a cyber operation against the hosted international organization. First this section looks at the right to respond and after at the different responses that can possibly be given.

5.2.1 Right to Respond

The principle of due diligence holds that states must take into consideration another state's rights when exercising sovereignty. In cyberspace, this holds that states should act in respect of cyber activities:

'(1) carried out by persons in their territory or where use is made of items or networks that are in their territory or which they otherwise control;

(2) that violate a right of another state; and

(3) whose existence they are, or should be, aware of.'

(Government of the Netherlands, 2019 as stated in the *Corfu Channel Case; Assessment of Compensation* (United Kingdom v. Albania), International Court of Justice, 1949).

It should be noted that not all states agree with this principle because this would impose accompanying obligations. Acting in due diligence is especially difficult since, as mentioned in section 5.1.2, the correct attribution poses technical difficulties and wrong attribution could result in legal consequences. However, the Netherlands does regard the principle of due diligence as an international obligation (Government of the Netherlands, 2019).

In addition, as stated in the Tallinn Manual 2.0 (Schmitt 2017), Rule 6:

'A State must exercise due diligence in not allowing its territory, or territory of cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.' (p.30.).

This could suggest that the hosting state has an obligation to prevent cyber operations conducted on its territory against the function of the international organization when the functioning also falls under the right of other states. A state may then exercise its jurisdiction over cyber activities according to Rule 8 of the Tallinn Manual 2.0 as long as it adheres to the boundaries set out by international law. This rule is closely related to the principle of sovereignty. A state has full jurisdiction over its territory, including the persons and objects in it. Therefore, when an offence occurs, the state in which it occurs has primary jurisdiction.

This is also closely linked to Rule 9 regarding territorial jurisdiction:

'A State may exercise territorial jurisdiction over: (a) cyber infrastructure and persons engaged in cyber activities on its territory; (b) cyber activities originating in, or completed on, its territory; or (c) cyber activities having a substantial effect in its territory.' (Schmitt, 2017, p.55.).

Rule 9 is similar to Rule 8 but is a necessary addition for cyber activities since these have the means to occur outside a state's territory yet have a significant effect on the territory of the victim state.

Digital developments have enabled states to act outside their territory whilst staying in their own borders. The non-intervention principle has derived from the sovereignty principle and holds that intervention with another state's internal or external affairs is not in accordance with international law. An example is the cyber operation in December, 2015, when the critical infrastructure of Ukrainian power was targeted, resulting in thousands of homes without electricity. This was in violation with international law. The main definition of interference is that the goal is change in behaviour of the targeted state (Government of the Netherlands, 2019). When a cyber activity is not in accordance with international law and the state is allowed to exercise its jurisdiction, it is up to the state to determine, given the circumstances, what the appropriate response would be (Government of the Netherlands, 2019).

In general, it can be concluded that the hosting state of an international organization either can argue a cyber operation to be infringing territorial or functioning sovereignty. The latter is not only an infringement of sovereignty of the hosting state, but all states supporting the international organization. In addition, the hosting state holds the responsibility to respond. This is further discussed in section 6.2.1.

5.2.2 Kind of Reponses

If a state does respond, there are several options of how a state can respond. These include: (1) retorsion, (2) countermeasures, (3) necessity and (4) self-defense (as mentioned in section 2.3). When acts are not in violation with international law but still undesirable, states are allowed to declare a person as a "persona non grata" (meaning an unwanted person). Another option is to take economic countermeasures or cutting off digital access in its territory. The Council stated that cyber operations with significant effect fall under the new sanctions' regime enforced in the European Union. It was not specified what significant effect entails. However, it was specified that member states should take the necessary measures to prevent entry or transit through its territory (Capparelli & Fratini, 2019).

Article 49 on Object and limits of countermeasures of the treaty of Responsibility of States for Internationally Wrongful Acts (2001), states that if an internationally wrongful act by another state is conducted, the victim state is allowed to take countermeasures. If countermeasures are taken, it is up to the victim state to invoke the other state's responsibility. This holds that the act can be attributed to the state and is recognized as a violation of international law. In addition, the victim state must notify the other state of the countermeasures being taken. These countermeasures should be proportionate (as stated in Article 51 on Proportionality), meaning that the gravity of the countermeasure should be in balance with the wrongful act committed against the state (United Nations, 2005).

Furthermore, an act of necessity is justified when the act would usually classify as wrongful in accordance with international law. However, this can only be invoked when there are serious consequences to the act committed against the concerning state. The response of necessity has no clear guidelines and is determined case-by-case. The origin of the damage does not have to be established as it mainly concerns the outcome which invokes the necessity of the response. An example of a consequence of a cyber operation which would lead to the response of necessity is when the financial market collapses (Government of the Netherlands, 2019). Self-defense is related to an armed attack which is not applicable to this thesis and will therefore not be discussed.

6. Analysis

This section provides an analysis of the application of the international laws (as presented in the previous Chapter) to the Organisation for the Prohibition of Chemical Weapons (OPCW) case (as explained in Chapter 4). First, the OPCW case itself is discussed to examine the legality of the operation as well as the sovereignty and attribution of the Netherlands to the Russian intelligence agency GRU. The second part looks at the legality of the response of the Netherlands to the OPCW case and the appropriateness taking into account the international laws and regulations.

6.1 International Law and the OPCW Case

This section examines the kind of cyber operation conducted by the GRU against the OPCW and whether or not this was in violation with international law. In addition, it is examined whether or not the sovereignty of the Netherlands was infringed or whether Russia was within its right to act. This also means looking at whether or not the correct attribution to the Russian military agency GRU was made. Last, it is discussed to what extent the international laws are applicable to the OPCW considering it is an international organization.

6.1.1 Cyber Operation

As mentioned in section 5.1.1, the legality of cyber operations is not dependent on the act itself, but rather on the effect it has. A harmful effect would entail damage or destruction (either physical or non-physical). For the OPCW case, the effect of the operation is not known. Before the GRU was able to conduct its cyber operation against the OPCW, it was stopped in timely manner by the MIVD without any (known) damage (Government of the Netherlands, 2018). Therefore, only the intended damage of the operation can be discussed.

In general, it is assumed that the GRU attempted to influence the investigations conducted against Russia regarding the poisoning of Russian double spy Sergei Skripal and his daughter, as well as the chemical attack on Douma. It would also not be the first investigation the GRU tried to intervene with. As mentioned in section 3.2.1.C, the investigation into MH17 was also victim of the GRU's interception. If the involvement of Russia can be proven, it could face proportionate sanctions. However, there was no prosecution regarding the operation against the investigation, but rather the shooting down of the Malaysian flight itself. Ank Bijleveld, the Dutch Minister of Defense, later brought to light that one of the operators who targeted the MH17 investigation was also present at the

OPCW. Furthermore, the equipment in the hired car could hack into the Wi-Fi network of the OPCW and the equipment was operational at the time of interception (Government of the Netherlands, 2018).

However, the cyber operation could also have been intended as a cyber espionage operation, which concerns solely the gathering or the attempt to gather information. There is no consensus on the legality of cyber espionage. It is not in violation with international law per se since it does not interfere with data. The legality depends on the method through which it is carried out (as discussed in section 5.1.1). The method of cyber espionage could be in violation with international law when force was used (Yoo, 2015). For the OPCW case, there was no (known) force used. Therefore, if the intent was cyber espionage, the operation would arguably not be in violation with international law.

Still, the activity was not allowed since no authorization was given to the GRU to conduct the cyber operation. In addition, it undermines the right to investigate. The government of the Netherlands (2018) even argued that it undermines the international rule of law. Whether or not the cyber operation was an infringement of sovereignty, is discussed in the following section. Both kinds of cyber operations, either to manipulate the investigation or espionage, are equally possible intents. However, for this thesis the first option is more interesting to examine. The legality of cyber espionage remains contested in international law and the operation does not have the possibility of influencing a specific effect (such as the ability to conduct inherently governmental functions). For the interest of addressing gaps in international law, the manipulation of the investigations is assumed to be the intent of the GRU for the OPCW cyber operation.

6.1.2 Sovereignty and Attribution

Whether or not the cyber operations against the OPCW was an infringement of sovereignty can be examined in two different ways. The first concerns the infringement of territorial sovereignty of the hosting state, in this case the Netherlands. The second way concerns the infringement of states' sovereignty who support the OPCW and for which the Netherlands holds due diligence to prevent cyber operations in its territory. An infringement of sovereignty will then occur if the cyber operation interferes with inherent governmental functions.

First is examined whether there was an infringement of territorial sovereignty of the hosting state, the Netherlands. Territorial sovereignty entails that a state has the right to

exercise jurisdiction over its own territory. The GRU did not get the authorization to conduct the cyber operation within the territory of the Netherlands (or at all). However, the effects of the cyber operation should be present on the territory of the hosting state. In the OPCW case, there was no physical damage (as far as is known). In addition, the network of the OPCW was targeted and not the Dutch territory. Therefore, one could argue that there was no infringement of territorial sovereignty of the Netherlands.

Secondly, it should be determined whether there was an infringement of the sovereignty of the states supporting the OPCW. This holds that inherently governmental functions can no longer be conducted. Inherent governmental functions have no legal definition. In general, they entail that only states may engage with them, for example conducting elections or conducting law enforcement database searches (Schmitt, 2019). To clarify, an inherently governmental function could be defined as:

'one that, as a matter of law and policy, must be performed by federal government employees and cannot be contracted out because it is "intimately related to the public interest".'

(Luckey, Grasso & Manual, 2009, p.1.).

In other words, an international organization which preforms oversight over specific functions performs inherently governmental functions. One could argue the OPCW is such an international organization. The OPCW was created at the Chemical Weapons Conventions (CWC) in 1997 to ensure the elimination of chemical weapons. The OPCW investigates whether or not chemical weapons were used in attacks. Furthermore, the OPCW cooperates with the United Nations on practical and policy issues (External Relations Division, 2000). The investigations are of public interest and important that these can be conducted without being undermined by third parties. The attempted cyber operation by the GRU could have undermined the investigations into the poisoning of Sergei Skripal and the chemical attack in Douma. As defined in section 2.1, cybersecurity for the Netherlands entails the prevention of disruption, damage or violation of integrity of information stored in ICT systems. One could argue that the case of the OPCW is of great importance to ensure cybersecurity. Therefore, if the cyber operation would have succeeded, one could argue it was an infringement of sovereignty of all supporting states. The question which then arises is whether the Netherlands, as hosting state, should be held responsible to have due diligence and respond to the operation. This will be discussed in section 6.2.1.

The attribution of the cyber operations against the OPCW holds that a state is held responsible for the action. This can be done either legally, politically and/or technically. It should also be examined whether or not the attribution is reliable. In the OPCW case, four GRU officers were present at the scene with the tools to enter the network of the OPCW. Therefore, the attribution to Russia can be made with a significant level of certainty. The act was made public by the government of the Netherlands and therefore political attribution was conducted. In addition, technical attribution shows that the equipment was able to conduct the cyber operation which the GRU brought by car. Last, legal attribution would entail that legal claims were made. A state can be held responsible, according to Rule 14 of the Tallinn Manual 2.0 when they have conducted an internationally wrongful act. Although, no legal claims were made, it could be considered that this might have been appropriate. However, the GRU officers travelled with diplomatic passports, therefore evicting the officers as unwanted persons, seems the most appropriate response in accordance with international law. This will be further discussed in section 6.2. It is not the first malicious cyber operation attributed to the GRU and perhaps can only be stopped when harsher measures are taken. In general, the main actors contributing to digital unpeace are intelligence agencies (Boeke, Broeders & Georgieva, 2019). Therefore, this case could set an example that these activities will and should not be tolerated since they arguably undermine the international rule of law.

6.1.3 International Organization

In general, international organizations do not fall under the scope of international law. However, the OPCW was created at the Chemical Weapons Convention (CWC). In April, 1997, the multilateral disarmament agreement against weapons of mass destruction was signed. This included the creation of the OPCW which consists of three main bodies: The Executive Council, Technical Secretariat and the Conference of the States Parties. The OPCW holds the responsibility to disarm and is supported by 193 states (External Relations Division, 2000). The OPCW is known to be an intergovernmental organization (IGO) as it became the implementing body after the Chemical Weapons Convention (CWC). This is due to the fact that it was created by treaties and is comprised primarily of member states. Therefore, IGOs do have an international legal personality and are an aspect of international law. Instead of national jurisdiction, legal mechanisms are enforced to ensure legal accountability (Matthew, 2010).

In Article 2 it is stated that the OPCW has a legal personality and can act, for example, in legal proceedings. The question which arises is whether the OPCW itself would be able to

respond to a cyber operation such as was conducted by the GRU in April, 2018. In general, having a legal personality entails that one can both sue and be sued, however, the OPCW has immunity from legal process, as stated in Article 4 (Conference of the States Parties, 1997). This also holds that the OPCW is able to sue the GRU with supposedly illegal cyber activities. However, considering that the operation was stopped by the MIVD and not the OPCW itself and the assumption that no damage was done, the responsibility of the response is more likely to be attributed to the hosting state than to the international organization targeted.

Furthermore, the legal agreement between the OPCW and the hosting state, the Netherlands (Conference of the States Parties, 1997), states in Article 6 that the Netherlands is responsible to act when necessary to ensure that the headquarters of the OPCW shall not be disposed in whole or in part. One could argue that the Wi-Fi network of the OPCW is a part of the OPCW headquarters itself. This means that the Netherlands was indeed responsible to ensure its safekeeping. The protection of the headquarters of the OPCW is set out further in Article 8 of the agreement. This article states that the Netherlands should exercise due diligence to ensure the security of the OPCW without it being impaired by other persons attempting to enter without the authority to do so. The operation of the GRU and their physical presence at the scene would fall under this scope, meaning that it was indeed the responsibility of the Netherlands to act. Therefore, the following section looks at the response of the hosting state, the Netherlands and its appropriateness in accordance with international law.

6.2 International Law and the Response to the OPCW Case

This section looks at international law and the right of the Netherlands as hosting state of the international organization OPCW to respond. In addition, the kind of response given is examined as well as other possible responses that could have been given to analyse whether or not the given response was appropriate (in accordance with international law).

6.2.1 Right to Respond

As noted in section 5.2.1, a state can act with due diligence when cyber operations affect a states' sovereignty. The previous sections discussed the legality of the cyber operations as well as whether or not it was an infringement of sovereignty, either of the hosting state or of the states supporting the international organization. Since due diligence is closely related to the principle of sovereignty, one could argue for both sides as to why the

response in due diligence would or would not be appropriate, in accordance with international law. If one looks at territorial sovereignty, this was not present for the OPCW case (as discussed in section 6.1.2). The GRU travelled to the OPCW with the equipment to get into the network of the OPCW. However, the Dutch Defense Intelligence and Security Service (the MIVD) was able to stop the operation before the network was affected. It is unlikely that the operation would have harmed the Dutch territory, as discussed in section 6.1.2. This also holds that the non-intervention principle, meaning that outside states can interfere, does not apply (Moynihan, 2019).

Still, the Dutch Minister of Defense, Ank Bijleveld, stated that the operation was internationally wrongful. She did not specify in what way. However, Ank Bijleveld did specify that the GRU's operation shows a geopolitical trend where state actors are exploiting digital vulnerabilities (Government of the Netherlands, 2018). In addition, the OPCW is supported by 193 states and holds the responsibility to prevent the creation and fabrication and use of chemical weapons. It would be the responsibility of the Netherlands to protect international organizations hosted within its border. She claims that this is what has been done (Schmitt, 2019). The other form of infringement of sovereignty, when the cyber operation targets the ability of the international organization to perform its inherent governmental functions, is argued to be applicable in the OPCW. This affected not only the Netherlands, but all 193 states supporting the OPCW. Therefore, it is argued that Rule 8 of the Tallinn Manual 2.0 (as discussed in section 5.2.1) applies. This rule allows the state within which its territory the cyber operation occurred to act with an appropriate response and in accordance with international law. Therefore, the Netherlands had the right to respond to the OPCW operation. The kind of response which could have been given and which was given, is discussed in the following section.

6.2.2 Kind of Response

The main response to the operation occurred on the day of the operation itself. When the Dutch military intelligence stopped the GRU's cyber operation, they escorted the officers present at the territory of the OPCW to the airport and they were evicted as unwanted persons, or in legal terms: personas non grata. This could be classified as a retorsion response and is in accordance with international law. Though no official statement was made, the Minister of Defense was asked about the operation in the talk show *WNL* which is broadcasted on NPO1, Dutch television. The answer to the question if the Netherlands is in a "cyberwar" with Russia was answered by Ank Bijleveld with a '*yes*'. She added that the nature of war has changed

and that the OPCW operation conducted in April, 2018, is an example thereof. Furthermore, the Minister of Defense stated to have offered NATO cyber soldiers to increase resilience as well as enable a more offensive response (Pieters, 2018). In general, foreign-intelligence agencies like the GRU are mischarged with cyberwar. As mentioned in the introduction, this would mean that there was a use of force and the operation would be labelled as a cyber-attack. Since this is not the case, this attribution would not be in accordance with international law (Boeke & Broeders, 2018). Still, there was no official war declared between Russia and the Netherlands, but rather a diplomatic argument made that these actions are not tolerated.

No further (legal) response was given, the question arises whether this was proportionate and appropriate, or if further retorsion, countermeasures, necessity or self-defense would have been better in accordance with international law. The operations conducted by the GRU are deemed to undermine the international rule of law. However, no real actions to prevent similar events in the future have been taken. This could be due to the fact that the applicability of international law in cyberspace remains vague and contested. Therefore, this thesis aims to provide a basis upon which further discussion can be held on the illegality of these operations and the appropriateness of the responses given.

7. Conclusion & Discussion

The final chapter provides the conclusion in which the research questions, as imposed in section 1.2, are answered. In addition, the discussion explains the limitations, implications and provides some suggestions for future research.

7.1 Conclusion

This section aims to give an answer to the research question as imposed in the introduction: *To what extent do state-sponsored cyber operations against international organizations violate international law?* To do so, the separate questions (as also presented in the introduction) are answered, followed by a general conclusion.

7.1.1 Research Question 1

The first question of this thesis is: *To what extent was the intended cyber operation against the OPCW in violation with international law?* To examine the legality of the operation, the effect of the operation, the infringement of sovereignty, the attribution and the applicability of international law to the international organization OPCW were examined. There was no known effect since the cyber operation was stopped in timely manner. The possible intent of the cyber operation is either cyber espionage or to influence the investigations on Russia's possible involvement in the poisoning of the double-spy Sergei and Yulia Skripal as well as the chemical attack in Douma. There could have been a significant effect since the tools present in the GRU's rented car allowed both intents. Still, for the purpose of filling the gaps in international law, the second option was assumed to have been the intent.

It was not an infringement of territorial sovereignty since there was no (likeliness of) physical effect on the Dutch territory. However, it could have been an infringement of sovereignty regarding the ability of the international organization to conduct its inherently governmental functions. This holds that an international organization is able to conduct oversight functions important to the public, such as safekeeping from chemical weapons, which is the case for the OPCW. Therefore, one could argue that the GRU cyber operation against the OPCW was an infringement of sovereignty of the 193 states supporting the OPCW.

Despite the fact that it remains unclear whether the OPCW itself could have legally responded to the operation; in the agreement between the hosting state and the OPCW, the

Netherlands is responsible for the safekeeping of the OPCW's headquarters. Therefore, the following section answers the research question regarding the response of the Netherlands.

7.1.2 Research Question 2

The second question of this thesis is: *To what extent is the response of the Netherlands to the OPCW cyber operation appropriate, in accordance with international law?* To examine this question, the right to respond of the Netherlands was examined as well as the kind of response. If one would argue that there was an infringement of sovereignty, as one could (as was shown in the previous section), the Netherlands has the right to respond. GRU's operation could have undermined OPCW's functioning. This affects the 193 supporting states and usually the hosting state holds the responsibility to act. The kinds of responses differ per case in appropriateness and proportionality. Therefore, it remains difficult to say if the response was appropriate.

However, the response to evict the GRU officers as unwanted persons, falls under a retorsion response and is in accordance with international law. Still, the question arises whether this was enough. As stated by the Dutch Minister of Defense at that time, these ongoing operations conducted by Russia could undermine the international rule of law. It could be argued that more offensive measures, as suggested by Ank Bijleveld, are necessary to truly prevent these cyber operations from happening. However, this can only be speculated in this case and therefore future research is necessary, as will be discussed in section 7.2.3.

7.1.3 Overall Conclusion

To answer the question: *To what extent do state-sponsored cyber operations against international organizations violate international law?*, the following can be concluded: the cyber operation of the OPCW itself is arguably an infringement of sovereignty as the operation could have affected the functioning of the international organization. This affects the 193 supporting states and it is usual that the hosting state bares the responsibility to protect and respond appropriately. The response of the hosting state, the Netherlands, of retorsion was in accordance with international law. To enable generalizations, further research is necessary as is discussed in the discussion section.

7.2 Discussion

The discussion section provides the limitations to this thesis which should be kept in mind. In addition, the academic and practical implications are discussed as well as suggestions for future research.

7.2.1 Limitations

One limitation to consider is that evidence provided in this thesis is gathered from online sources. The sources were evaluated on reliability, however, there is no complete certainty that the whole and correct evidence has been provided since it is not always of interest to disclose information publicly on cyber operations. In addition, since the cyber operation was stopped pre-emptively, only the intent of the cyber operation can be discussed. In particular, the fact that the GRU cyber operation was conducted in response to the investigations that were conducted regarding the involvement of Russia, is a speculation based on likeliness. This has not been confirmed by the GRU.

Furthermore, as mentioned in section 3.3.1, data is not always available since states are not keen to inform other states of their cyber capabilities. Since the Netherlands decided to publicly out the cyber operation, more information is present. However, this does not mean that other relevant information is not held back to prevent Russia from being able to take certain measures into account when conducting another cyber operation. Last, this thesis examines a specific case and is only the first step. There is a bigger issue at stake regarding the lack of clarity in the application of international law in cyberspace. The need for further research is discussed in section 7.2.3.

7.2.2 Implications

This thesis has shown that the cyber operation of the GRU could be argued as an infringement of sovereignty and that the response of the hosting state was in accordance with international law. The importance of this thesis is further discussed through the academic and practical implications.

7.2.2.A Academic Implications

This thesis is of academic relevance because it looked at the existing gaps in international law and documents. It is established that cyber operations conducted against international organizations are in violation with international law since they are arguably an infringement of a states' sovereignty. The hosting state is then often responsible to respond to cyber operations conducted against international organizations on that state's territory.

However, the gaps in international law continue to exist when they are not researched and covered in scholarly work.

As mentioned in the introduction, there are still grey zones in international law with regard to cyberspace. This thesis is a start to filling those gaps. Important international documents, such as the EU Cyber Diplomacy Toolbox (Moret & Pawlak, 2017), lack information on the applicability to international organizations. In the other cases, besides the OPCW, such as the IAEA, WHO and the UN (as presented in Chapter 3), international organizations are also victim of cyber operations. Therefore, scholars need to continue looking into this as well as the responses that are given by the hosting states or by the international sphere in general. In particular, scholars need to examine what type of response could have the necessary effect of preventing international organizations from being a victim of cyber operations.

7.2.2.B Practical Implications

Even though there is a gap in international law, this thesis explained how the cyber operation conducted by the GRU undermines international law. There is also a practical relevance which policy makers should take into account.

As mentioned in the introduction, cyber operations that are identified as 'below-the-threshold' operations can cause damage to infrastructures or, as shown in this thesis, endanger the governmental functioning of organizations. It is important that policy makers take into account that these cyber operations violate international law to ensure that cyberspace is secured. In particular, the GRU was already on the radar of the MIVD before they travelled to the OPCW to conduct a cyber operation. It should be researched whether states could legally act before these state-sponsored actors are given the change to operate. In general, international law focusses on the effect of the operation rather than on the operation itself (as mentioned in Chapter 5). This holds that one can only continue with legal proceedings when there was an effect, making it more difficult to act preventively or when the operation, such as the OPCW case, was stopped on time. This should be reconsidered by policy makers to enable preventive actions.

Even though it is established that cyber operations could be in violation with international law, the responses of the states have proven insufficient since cyber operations similar to the OPCW case continue to be conducted. To protect the information stored in cyberspace, or in other words to ensure cyber and information security, policy makers should

look into appropriate measures and sanctions which could be taken to prevent international organizations from becoming a victim of cyber operations. Still, future research is needed to establish what would be defined as “appropriate measures and sanctions”.

7.2.3 Future Research

This thesis is a mere beginning of evaluating the applicability of international law regarding cyberspace, therefore, future research suggestions are provided. Russia does not refer to cyber security but rather information security, as pointed out in section 2.1. Information is an important asset in cyberspace, but also in particular in cyberwar. The question arises whether information warfare could be applicable in the violation of investigations and if the law of warfare would apply.

Also, it remains unclear whether or not the response of the Netherlands was sufficient to prevent future operations that undermine the international rule of law from reoccurring. It is questionable if a small country, like the Netherlands, is able to stop operations conducted by great powers such as Russia. Therefore, one could research whether or not more offensive responses are necessary with a focus on politics rather than law.

In addition, similar cases, as presented in section 3.1 showed that there were little to no responses. One could look at why this was the case and to what extent it was proportionate and effective or if political relations played part in the (absence of the) response. Furthermore, as mentioned in section 6.2.2, the response of the Dutch Minister of Defense Ank Bijleveld to out GRU’s operation and say that this situation could be identified as cyberwar, is a diplomatic response. Rather than legal responses, the focus in future research could lie on the appropriateness and effect of diplomatic responses. The Clingendael Policy Brief (van der Meer, 2015) describes the widely varying governmental responses and policy instruments used to cyber operations. This brief also states that more research should be conducted to look at the prevention of cyber operations. One could therefore look into this further by examining the OPCW case or other similar cases.

Last, this thesis is a single case study of the OPCW. Future research could look at the responsibility of states to respond to cyber operations conducted against international organization in other similar cases. This could either verify the conclusion of this thesis or provide a different point of view upon which new research proposals can be provided.

To conclude, in the Statute of the International Court of Justice (2020), Article 38(1)(d), the following is stated regarding scholarly work: *'teachings of the most highly*

qualified publicists of the various nations' are also among the 'subsidiary means for the determination of the rules of law'. Scholarly work is essential for developing treaties and rules. Therefore, it is important to continue researching the application of international law in cyberspace.

References

Adams, M. & Reiss, M. (2018). International Law and Cyberspace: Evolving Views. *Cybersecurity and Deterrence.* Retrieved from https://www.lawfareblog.com/international-law-and-cyberspace-evolving-views

Algemene Inlichtingen- en Veiligheidsdienst (2018). Jaarverslag AIVD 2018. *AIVD.* Retrieved from https://www.aivd.nl/documenten/jaarverslagen/2019/04/02/jaarverslag-aivd-2018

Barros, A.S., Ryngaret, C. & Wouters, J. (2016). International Organizations and Member State Responsibility: Critical Perspectives. *Brill Nijhoff's journal International Organizations Law Review.* Retrieved from https://lccn.loc.gov/2016026751

BBC (2018). How the Dutch Foiled Russian 'Cyber-Attack' on OPCW. *BBC News.* Retrieved from https://www.bbc.com/news/world-europe-45747472

BBC (2018). Russian Spy: What Happened to Sergei and Yulia Skripal? *BBC News.* Retrieved from https://www.bbc.com/news/uk-43643025

Boeke, S. & Broeders, D. (2018). The Demilitarisation of Cyber Conflict. *Survival, 60(6),* p.73-90. Doi: 10.1080/00396338.2018.1542804

Boeke, S,. Broeders, D. & Georgieva, I. (2019). *Foreign Intelligence in the Digital Age: Navigating a State of 'Unpeace'*. The Hague Program for Cyber Norms Policy Brief. September 2019.

Buchan, R. & Navarrete, I. (2019). Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions. *Corenell International Law Journal, 51(4),* p. 897-953. Retrieved from https://heinonline-org.ezproxy.leidenuniv.nl:2443/HOL/Page?lname=&public=false&collection=journals&handle=hein.journals/cintl51&men_hide=false&men_tab=toc&kind=&page=897

Capparelli, F. & Fratini, A. (2019). European Union Introduces New Economic Sanctions Against Cyber Attacks. *Lexology: ICT Legal Consulting.* Retrieved from https://www.lexology.com/library/detail.aspx?g=69f052d3-a8ec-44b3-880f-e3805f9d0c66

CBSNews (2018). Russia Accuses the U.K. of Staging Fake Chemical Attack in Syria. *CBSNews.* Retrieved from https://www.cbsnews.com/news/russia-accuses-uk-of-staging-fake-chemical-attack-syria/

Collins, A. (2016). *Contemporary Security Studies.* Oxford: Oxford University Press. Fourth Edition.

Conference of the States Parties. (1997). Decision: OPCW Headquarters Agreement. *C-I/DEC.59.* Retrieved from https://www.opcw.org/sites/default/files/documents/CSP/C-I/en/C-I_DEC.59-EN.pdf

Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2000). The Concept of Cyber Security Strategy of the Russian Federation. *CCDCOE.* Retrieved from https://ccdcoe.org/library/strategy-and-governance/?category=cyber-security-strategies

Council on Foreign Relations (2020). Cyber Operations Tracker. *CFR.* Retrieved from https://www.cfr.org/interactive/cyber-operations#CyberOperations

Crerar, P., Henley, J. & Wintour, P. (2018). Russia Accused of Cyber-Attack on Chemical Weapons Watchdog. *The Guardian.* Retrieved from https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body

Cybersecuritybeeld Nederland (2018). CSBN 2018. *National Coördinator Terrorismebestrijding en Veiligheid: Ministerie van Justitie en Veiligheid.* Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2018/06/13/tk-bijlage-cybersecuritybeeld-nederland-csbn-2018

Delerue, F. (2019). Reinterpretation or Contestation of International Law in Cyberspace. *Israel Law Review, 53(3),* p.295-326. Doi: 10.1017/S0021223719000104

Delerue, F. (2020). *Cyber Operations and International Law.* London: Cambridge University Press.

The Department of Defence (2020). DOD Dictionary of Military and Associated Terms. *DoD.* Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

Department of Justice (2018). U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations. *The United States*

Department of Justice. Retrieved from https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

Eichensehr, K. (2020). The Law & Politics of Cyberattack Attribution. *UCLA Law Review, 76,* p19-36. Retrieved from https://www.law.uchicago.edu/files/2019-11/lpa_draft_11-19-19.pdf

External Relations Division (2000). The Chemical Weapons Convention and the OPCW - How They Came About: Fact Sheet 1. *OPCW.* Retrieved from https://www.opcw.org/sites/default/files/documents/publications/fact_sheets/01.pdf

Forcese, C. (2016). Pragmatism and Principle: Intelligence Agencies and International Law. *Virginia Law Review, 67(102).* Retrieved from https://www.virginialawreview.org/volumes/content/pragmatism-and-principle-intelligence-agencies-and-international-law

Gaja, G. (2006). Responsibility of International Organizations. *United Nations.* Fourth Report. Retrieved from https://legal.un.org/ilc/documentation/english/a_cn4_564.pdf

Gisel, L. & Olejnik, L. (2018). The Potential Human Cost of Cyber Operations. *International Committee of the Red Cross.* Retrieved from https://www.icrc.org/en/publication/potential-human-cost-cyber-operations

Goud, N. (2020). Russia Hacked MH17 Investigation in Malaysia. *Cybersecurity Insiders.* Retrieved from https://www.cybersecurity-insiders.com/russia-hacked-mh17-investigation-in-malaysia/

Government of the Netherlands (2017). International Cyber Strategy. *Government of the Netherlands.* Retrieved from https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy

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

Government of the Netherlands (2019). Appendix: International Law in Cyberspace. *Government of the Netherlands.* Retrieved from

https://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwimgpiStaHpAhVRjqQKHf7VBYIQFjAAegQIAhAB&url=https%3A%2F%2Fwww.government.nl%2Fbinaries%2Fgovernment%2Fdocuments%2Fparliamentary-documents%2F2019%2F09%2F26%2Fletter-to-the-parliament-on-the-international-legal-order-in-cyberspace%2FInternational%2BLaw%2Bin%2Bthe%2BCyberdomain%2B-%2BNetherlands.pdf&usg=AOvVaw1KHhRucQjobo_Sb6LcGS1i

Granova, A. & Slaviero, M. (2017). Cyber Warfare. *ScienceDirect.* Retrieved from https://www.sciencedirect.com/topics/computer-science/cyber-operation

International Court of Justice (1949). *Corfu Channel Case; Assessment of Compensation (United Kingdom v. Albania).* The International Court of Justice. Retrieved from https://www.icj-cij.org/en/case/1

International Court of Justice (2020). Statute of the International Court of Justice. *ICJ.* Retrieved from https://www.icj-cij.org/en/statute

International Law Commission. (2020). Articles on State Responsibility. *International Committee of the Red Cross.* Retrieved from https://casebook.icrc.org/case-study/international-law-commission-articles-state-responsibility

Irwin, L. (2018). Do You Know the Difference Between Cyber Security and Information Security? *ItGovernance.* Retrieved from https://www.itgovernance.co.uk/blog/do-you-know-the-difference-between-cyber-security-and-information-security

Kamer, F.D., Starr, S.H., Wentz, L.K. (2009). *Cyberpower and National Security.* Washington, D.C.: Potomac Books. ISBN: 9781597974233. 9781597979337.

Kelley, M.B. (2012). Report: Anonymous Hacks Top Nuclear Watchdog Again to Force Investigation of Israel. *Business Insider.* Retrieved from https://www.businessinsider.com/anonymous-hack-iaea-nuclear-weapons-israel-2012-12?international=true&r=US&IR=T

Klabbers, J. (2017). *International Law*. Cambridge: Cambridge University Press. Second Edition.

Kremling, J. & Parker, A.M.S. (2017). Cyberspace, Cybersecurity, and Cybercrime. *SAGE publications.* Retrieved from https://books.google.nl/books?id=I39ZDw AAQBAJ&pg=PT28&hl=nl&source=gbs_toc_r&cad=3#v=onepage&q&f=false

van Leeuwen (2018). Big Russian Cyber Attack Against the OPCW in The Hague Foiled – 4 Russians Expelled. *DutchReview.* Retrieved from https://dutchreview.com/news/ international/big-russian-cyber-attack-against-the-opcw-in-the-hague-foiled-4-russians-expelled/

Lotrionte, C. (2018). Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law. *The Cyber Defense Review, 3(2),* p.73-114. Retrieved from https://www.jstor.org/stable/26491225?seq=1#metadata_info_ tab_contents

Luckey, J.R., Grasso, V.B. & Manuel, K.M. (2009). Inherently Governmental Functions and Department of Defense Operations: Background, Issues and Options for Congress. *Congressional Research Service.* Retrieved from https://fas.org/sgp/crs/misc/R40641.pdf

Maruyama, G & Ryan, C.S. (2014). *Research Methods in Social Relations.* Eighth edition. WILEY Blackwell, United Kingdom: Oxford.

Matthew, P. (2010). An Essay on the Accountability of International Organisations. *International Organizations Law Review, 7(2),* p.277-342. Doi: 10.1163/157237410X543332

van der Meer, S. (2015). Foreign Policy Responses to International Cyber-Attacks: Some Lessons Learned. *Clingendael.* Retrieved from https://www.clingendael.org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf

van der Meer, S. (2018). State-Level Responses to Massive Cyber-Attacks: A Policy Toolbox. Clingendael*; Netherlands Institute of International Relations.* Retrieved from https://www.clingendael.org/sites/default/files/2018-12/PB_cyber_responses.pdf

Mebius, D. (2018). Hoe Wist de MIVD Een Russische Hackpoging te Verijdelen? Een Reconstructie van Aankomst tot Aanhouding. *De Volkskrant.* Retrieved from https://www.volkskrant.nl/nieuws-achtergrond/hoe-wist-de-mivd-een-russische-hackpoging-te-verijdelen-een-reconstructie-van-aankomst-tot-

aanhouding~b8af00c8/?utm_source=link&utm_medium=app&utm_campaign=shared%20content&utm_content=free

Ministerie van Defensie (2018). Jaarverslag MIVD 2018. *MIVD.* Retrieved from https://www.defensie.nl/downloads/jaarverslagen/2019/04/30/jaarverslag-mivd-2018

Ministerie van Defensie (2018). MIVD Verstoort Russische Cyberoperatie bij de Organisatie voor het Verbod op Chemische Wapens. *Defensie.* Retrieved from https://www.defensie.nl/actueel/nieuws/2018/10/04/mivd-verstoort-russische-cyberoperatie-bij-de-organisatie-voor-het-verbod-op-chemische-wapens

Modderkolk, H. (2019). Het is Oorlog Maar Niemand die het Ziet. *Uitgeverij Podium, Amsterdam.*

Moes, G. (2018). De Cyberoorlog Met Rusland is een Feit. Maar wat Betekent dat Precies?. *Trouw*. Retrieved from https://www.trouw.nl/nieuws/de-cyberoorlog-met-rusland-is-een-feit-maar-wat-betekent-dat-precies~b2bfd5e3/

Moret, E. & Pawlak, P. (2017). The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime? *European Union Institute for Security Studies.* Retrieved from https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf

Moynihan, H. (2019). The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention. *The Royal Institute of International Affairs.* Retrieved from https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf

Muncaster, P. (2020). NCSC: Russia's GRU to Blame for DNC and Other Attacks. *Info-Security Magazine.* Retrieved from https://www.infosecurity-magazine.com/news/ncsc-russias-gru-blame-dnc-other/

National Coordinator for Security and Counterterrorism (2019). Cyber Security Assessment Netherlands: CSAN 2019. *Ministry of Justice and Security*. Retrieved from https://www.thehaguesecuritydelta.com/media/com_hsd/report/255/document/CSBN2019-EN-def-Web-01-tcm32-405804.pdf

Nationaal Cyber Security Centrum (2013). Cyber Security Perspectives 2013. *Ministerie van Veiligheid en Justitie.* Retrieved from https://www.thehaguesecuritydelta.com/media/com_hsd/report/15/document/Cyber-Security-Perspectives-2013.pdf

Nettles, R.A., Merulla, C. & Warzala, S. (2019). Data Manipulation. *Cyber Security & Information Systems Information Analysis Center.* Retrieved from https://www.csiac.org/csiac-report/data-manipulation/

Ng, A. (2018). US Charges 12 Russian Hackers Tied to DNC Cyberattacks. *CNET.* Retrieved from https://www.cnet.com/news/us-charges-12-russian-hackers-tied-to-dnc-cyberattack/

North Atlantic Treaty Organization (2016). Warsaw Summit Communiqué. *NATO.* Retrieved from https://www.nato.int/cps/en/natohq/official_texts_133169.htm

North Atlantic Treaty Organization (2018). Statement by NATO Secretary General Jens Stoltenberg on Russian Cyber Attacks. *NATO.* Retrieved from https://www.nato.int/cps/en/natohq/news_158911.htm

Nye, J.S. (2011). *The Future of Power.* Public Affairs: New York.

Openbaar Ministerie (2020). Strafrechtelijk Onderzoek door Joint Investigation Team (JIT). *Openbaar Ministerie.* Retrieved from https://www.om.nl/onderwerpen/mh17-vliegramp/strafrechtelijk-onderzoek-mh17-jit

OPCW (2018). OPCW Spokesperson's Statement on Cyber Security. *Organisation for the Prohibition of Chemical Weapons, News.* Retrieved from https://www.opcw.org/ media- centre/news/2018/10/opcw-spokespersons-statement-cyber-security

Pieters, J. (2018). Netherlands in "Cyber War" with Russia, Defense Minister Says. *NLTimes.* Retrieved from https://nltimes.nl/2018/10/15/netherlands-cyber-war-russia-defense-minister-says

Rijksoverheid (2018). Nederlandse Cybersecurity Agenda: Nederland Digitaal Veilig. *Rijksoverheid.* Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/ 2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig

Rijksoverheid (2018). Wereldwijd voor een Veilig Nederland – Geïntegreerde Buiteland- en Veiligheidsstrategie 2018-2022. *Rijksoverheid.* Retrieved from https://www.rijksoverheid.nl/actueel/nieuws/2018/03/20/wereldwijd-voor-een-veilig-nederland---geintegreerde-buitenland--en-veiligheidsstrategie-2018-2022

Roberts, D. (2015). Obama Imposes New Sanctions Against North Korea in Response to Sony Hack. *The Guardian.* Retrieved from https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview

Robson, C. (1993). *Real World Research: A Resource for Social Scientists and Practitioner-Researchers.* Oxford: Blackwell.

Reuters (2007). Hackers did not Steal Sensitive Nuclear Information. IAEA. *Reuters.* Retrieved from https://www.reuters.com/article/net-us-nuclear-iaea-hacking/hackers-did-not-steal-sensitive-nuclear-information-iaea-idUSBRE8AQ0ZY20121129

Sanders-Zakre, A. (2018). Russia Charged With OPCW Hacking Attempt. *Arms Control Association.* Retrieved from https://www.armscontrol.org/act/2018-11/news/russia-charged-opcw-hacking-attempt

Satter, R., Stubbs, J. & Bing, C. (2020). Hackers Tried to Infiltrate the World Health Organization, the Latest in a String of Cyberattacks Aimed at Health Officials During the Coronavirus Pandemic. *Business Insider.* Retrieved from https://www.businessinsider.com/world-health-organization-hack-tried-steal-passwords-with-fake-website-2020-3?international=true&r=US&IR=T

Schmitt, M. (2019). The Netherlands Release a Tour de Force on International Law in Cyberspace: Analysis. *Just Security.* Retrieved from https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/

Schmitt, M.N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York: United States Naval War College: Cambridge Press.

Schmitt, M.N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* New York, United States Naval War College: Cambridge Press.

Therrien, A. & Roxby, P. (2018). Russian Spy: What are Nerve Agents and What do They do? *BBC News.* Retrieved from https://www.bbc.com/news/health-43328976

Tsakanyan, V.T. (2017). The Role of Cybersecurity in World Politics. *Vestnik RUDN; International Relations, 17(2),* p.339-348. Doi: 10.22363/2312-0660-2017-17-2-339-348

United Nations (2005). Responsibility of States for Internationally Wrongful Acts: 2001. *Legal United Nations.* Retrieved from https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

United Nations (2011). Report of the International Law Commission on the Work of its Sixty-third Session: Draft Articles on the Responsibility of International Organizations, with Commentaries. *Legal United Nations.* Retrieved from https://legal.un.org/ilc/texts/instruments/english/commentaries/9_11_2011.pdf

United Nations (2018). The Application of International Law in Cyberspace: State of Play. *Legal United Nations.* Retrieved from https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/

United Nations Security Council (2020). Purposes and Principles of the United Nations. *UNSC.* Retrieved from https://www.un.org/securitycouncil/content/purposes-and-principles-un-chapter-i-un-charter#rel2

The United States Department of Justice (2018). U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations. *The United States Government.* Retrieved from https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

VOANews (2020). Leaked Report Shows United Nations Suffered Hack. *Silicon Valley & Technology.* Retrieved from https://www.voanews.com/silicon-valley-technology/leaked-report-shows-united-nations-suffered-hack

Weaver, M. (2015). MH17 Crash Report: Dutch Investigators Confirm Buk Missile Hit Plane – Live Updates. *The Guardian.* Retrieved from https://www.theguardian.com/world/live/2015/oct/13/mh17-crash-report-ukraine-live-updates

Winder, D. (2020). United Nations Confirms 'Serious' Cyberattack with 42 Core Servers Compromised. *Forbes.* Retrieved from https://www.forbes.com/sites/daveywinder/2020/01/30/united-nations-confirms-serious-cyberattack-with-42-core-servers-compromised/#4bb20b4e633d

Wintour, P. & McKernan, B. (2020). Inquiry Strikes Blow to Russian Denials of Syria Chemical Attack. *The Guardian.* Retrieved from https://www.theguardian.com/world/2020/feb/07/inquiry-strikes-blow-to-russian-denials-of-syria-chemical-attack

Yin, R. (2018). *Case Study Research: Design and Methods.* Sage: Thousand Oaks.

Yoo, C.S. (2015). Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures. *University of Pennsylvania Law School.* Retrieved from https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2541&context=faculty_scholarship