North Korea, Iran & Saudi Arabia

Restrained in cyberspace or a threat to international peace?

By Marina Bindary

Master's Thesis - Spring 2019
Birthdate: 10.10.1989
Supervisor: Jan Lemnitzer
Political Science, University of Southern Denmark

Strokes: 179.122

Content

Resumé

Specialets titel er *Nordkorea, Iran og Saudi-Arabien – Selvbeherskede i cyberspace eller en trussel mod international fred?*

Cyberspace kan betragtes som et relativt nyt domæne, hvor konflikter mellem stater udspiller sig i gradvist større omfang og med nye teknologiske og virtuelle midler, der har et stort potentiale for ødelæggelse.

Traditionelle slyngelstater som Nordkorea og Iran, såvel som politisk kontroversielle stater som Saudi-Arabien – der opfattes som en allieret i Vesten – har med deres adfærd i cyberspace bidraget til en frygt for, at de nye magtmuligheder i det virtuelle domæne gør økonomisk udfordrede og politisk afsondrede stater modigere og dermed mere aggressive.

Jeg søger gennem dette speciale at bidrage til en forståelse af, hvordan stater som Nordkorea, Iran og Saudi-Arabien opfører sig i lyset af de nye magt-muligheder i cyberspace. Følgende forskningsspørgsmål søges dermed besvaret: Er hhv. Nordkoreansk, Iransk og Saudi-Arabisk adfærd i cyberspace karakteriseret ved selvbeherskelse, eller udgør de tre stater en trussel mod international fred?

De udvalgte cases i specialet er cyberangrebet på Sony Pictures Entertainment (SPE) i 2014 som eksempel på Nordkoreas adfærd, angrebet på Saudi Aramco i 2012 der eksemplificerer Irans opførsel i cyberspace samt sagen omkring Jamal Khashoggi i 2018 som repræsenterer Saudi-Arabiens adfærd i det virtuelle domæne. Der anvendes en deduktiv tilgang til undersøgelsen, hvis udgangspunkt er Cyber Restraint Theory's antagelse om, at cyberangreb der finder sted som et led i staters interaktion med hinanden i cyberspace, vil være begrænset i omfang og virkning, fordi stater frygter eskalering. Med andre ord, antages stater at være tilbageholdende i cyberspace, fordi de frygter at en aggressiv opførsel vil føre til konsekvenser uden for cyberspace. Denne hypotese testes ved at undersøge omfanget og virkningen af de nævnte tre cyberangreb, hvorefter der konkluderes på, om angrebene faktisk afspejler de tre staters generelle adfærd i cyberspace, samt om denne adfærd afspejler tilbageholdenhed i cyberspace.

Metodisk baserer undersøgelsen sig på processtracing. Her bliver Cyber Restraint Theory's begreber 'omfang' og 'virkning' gjort målbare ved at inddrage Friedrich Glasls konflikteskalationsteori.

Analysen af angrebet på SPE viser, at på trods af de materielle tab, der fulgte med angrebet, afspejler cyberangrebet en vis selvbeherskelse, idet omfanget og virkningen af angrebet kunne beskrives ved et af de laveste konfliktstadier i Glasls eskalationsteori. Desuden lod angrebet til at være udtryk for desperation efter at det mislykkedes Nordkorea at standse frigivelsen af filmen *The Interview* ved at rette sin klage til FN, og dermed ikke et udtryk for cyberkrigsførelse.

Angrebet på Saudi Aramco afspejler imidlertid en højere grad af konflikt, idet angrebet lader til at være et forsøg at påvirke Saudi-Arabiens olieproduktion og dermed landets økonomisektor samt grundlaget for dets internationale indflydelse. Konflikten eskalerede imidlertid ikke yderligere, og selvom der også i denne case var store materielle tab, så inddæmmede det saudiarabiske olieselskab konflikten hurtigt.

Endelig afspejlede sagen omkring mordet på Jamal Khashoggi et af Glasls højeste konfliktstadier, idet angrebet kostede et menneskeliv, konflikten eskalerede voldsomt rent politisk og den fremprovokerede en debat omkring definitionen af staters suverænitet i cyberspace.

Konklusionen på forskningsspørgsmålet er, at ikke alle cyberangrebene kan karakteriseres som cyber-selvbeherskelse og at såfremt der ikke inden for de kommende år opnås enighed om internationale love eller normer vedr. cyberspace, så kan specielt Iran og Saudi-Arabiens adfærd i det virtuelle domæne blive problematisk og potentielt udfordre den internationale fred, fordi sammenstødet mellem ikke-vestlige værdier og liberale demokratiske værdier i høj grad er mærkbar i cyberspace pga. de skader, der kan udrettes med få midler.

1. Introduction

Since cyber conflict is a relatively new international issue, the academic literature in the field is in many ways also in its infancy. It has repeatedly been pointed out that cyberspace is a new arena, where states that do not have conventional power in the form of military or economic resources can play a more significant role, because cyber action does not require much in the form of military or economic resources. In other words, economically challenged and politically shunned countries – like rogue and controversial states – can allegedly "punch above their weight" in cyberspace.

While research has been conducted on the cyber motives of traditional rogue states like North Korea and Iran, respectively, little effort has been dedicated to examining whether they pose a serious threat in cyberspace. This means that further research is needed to understand whether rogue and politically controversial states have free reign and more power opportunities in cyberspace – in other words, whether the new opportunities for aggression, presented by cyberspace, encourage states to act in a bolder manner than outside of the virtual domain. Since theories are still scarce in the field of cyber conflict, there is a need to understand whether new opportunities in cyberspace embolden traditionally weak states – in terms of economy and international influence – as well as politically controversial regimes to pursue a more aggressive policy, or whether their actions in cyberspace are restrained.

It is an interesting topic that I wish to contribute to through this thesis, because it potentially upsets the conventional understanding of rogue and controversial states, their objectives and the level of threat they pose to international peace. Furthermore, cyber conflict is the reality for many countries today, and several states have described the threat from cyber attacks as the number one threat facing them (e.g. Danish Defence Intelligence Service 2019; Garamone, 2018). Attacks like the one on the Saudi oil company Saudi Aramco, the hacking of Sony Pictures Entertainment, and the assassination of Saudi activist Jamal Khashoggi, respectively, have led to growing fears that Iran, North Korea, and Saudi Arabia – that is traditionally considered an ally of the West – are becoming bolder in their political pursuits due to the problems of attribution in cyberspace. An examination of the severity and impact of rogue states' conduct in cyberspace would thus shed light on potential dangers and contribute to an understanding of how states behave in cyberspace given the new power opportunities at their disposal.

1.1. Research question

This thesis is a contribution to the literature about cyber conflict, and it seeks an understanding of whether rogue and controversial states are aggressive or whether they are restrained in cyberspace.

Thus, my research question is the following: Is North Korean, Iranian and Saudi Arabian conduct in cyberspace characterized by restraint or do these states pose a threat to international peace?

Accordingly, my analysis will revolve around the question of how rogue and controversial states conduct themselves in cyberspace, which is examined by exploring how three cases – North Korea, Iran and Saudi Arabia behave in this domain. I will then go on to discuss whether the cases show cyber restraint or pose a threat to international peace.

1.2. Outline

This thesis is built around ten chapters:

Chapter 1 is an introduction containing my research question.

Chapter 2 contains a literature review.

Chapter 3 describes the theory that is the foundation of my analysis.

Chapter 4 presents an operationalization of the theory and of key concepts.

Chapter 5 presents ontological and epistemological assumptions.

Chapter 6 describes the methodology of this thesis.

Chapter 7 provides a brief description of the general conduct of North Korea, Iran and Saudi Arabia in cyberspace.

Chapter 8 contains analyses of the three selected cases; the chapter is divided into three subsections that each contain an analysis of one cyber attack, an interim conclusion, and a discussion of whether the selected cyber attack is representative of the general conduct of the respective state in cyberspace.

Chapter 9 is a discussion of whether North Korea, Iran and Saudi Arabia pose a threat to international peace.

Chapter 10 contains the conclusion to my research question.

2. Literature review

A clear and concise understanding of the central aspects of cyber conflict is vital in order to delimitate what is being examined in this thesis as well as avoiding misunderstandings. This is especially true for cyber-related terminology, which is still in its infancy and therefore still characterized by much ambiguity. As Valeriano and Maness point out: "… the mismanagement of terms by academics, the media, and policymakers can feed into the cyber hype.." (2015: 28). It is easy to imagine that the lack of clarity might contribute to the hype over cyber incidents, which largely characterizes the cyber security discourse at this point. As Valeriano and Maness put it: "We are now at the point where someone guessing at a Twitter password is classified by the media as a hack who has committed an act of cyber war." (2015: 22). When what might have been described as a 'cyber conflict' is labeled 'cyber war', a dangerous escalation is indicated and a discourse that is highly characterized by war terminology might affect how states choose to react in cyberspace.

Thus, the following is an elaboration of how the four central concepts are defined in the academic literature and how they are utilized in this thesis.

2.1. Rogue states (entities)

The term 'rogue states' is the cause of much political as well as academic debate. Wagner, Werner and Onderco (2014) define the term from three different perspectives, thus offering various understandings: "… from a traditional, state-centric view, states become 'rogues' if they attempt to acquire and proliferate Weapons of Mass Destruction and threaten their neighbors with the use of force. Proponents of a 'human security' perspective would instead emphasize the actual harm done to their own citizens in addition to the potential use of force against other states. Yet others would highlight the support of terrorism as a defining feature of 'rogue states.'" (2014: 5).

In accordance with Wagner, Werner and Onderco's account, according to Klare (1995), 'rogue states' were defined in the 1990s as states that possessed WMDs (1995: 27–28), and later as states that supported terrorism (Tanter, 1998), and "most recently, the policies of the pursuit of WMDs and support of terrorism were reaffirmed as important identifiers of rogues..." (O'Reilly, 2007).

Based on the above, in this thesis, rogue states are not merely defined as states that seek Weapons of Mass Destruction (WMD), but as states that are consistent with any of three definitions outlined

by Wagner, Werner and Onderco (2014), Klare (1995), Tanter (1998) and O'Reilly (2007). Thus, a state is considered rogue, if it seeks WMD, if it inflicts harm on its own citizens or if it supports terrorism. Based on this definition, not only North Korea and Iran are considered rogue states, but also Saudi Arabia, since harmful measures are taken against its own citizens in an attempt to subdue political unrest (this is further elaborated in the analysis of Saudi Arabia).

2.2. Cyberspace (domain)

Cyberspace is a relatively new domain in which nation-states, among other players, fight their power struggles (McGuffin and Mitchell, 2014; Lynn, 2010; Saalman, 2017; Pellerin, 2010 and more). It is furthermore a domain that has been subject to considerable disagreement in academic circles about how it can be best defined (e.g. Reardon and Choucri, 2012; Ottis and Lorents, 2011; Nye, 2010). Accordingly, more than one definition has been offered, but essentially many definitions mainly agree that cyberspace is a global network that connects different technological devices, and where information and ideas are exchanged not only between states, but also individuals (Reardon and Nazli, 2012; Nye, 2010; Kuehl, 2009).

Robert Reardon and Nazli Choucri describe cyberspace as a "… 'network of networks'… a global arena of interaction for countless shared activities and the exchange of information and ideas by people around the world… on a daily basis. It is now common to speak of the sum of these connections among computing and communications devices as a single, shared virtual domain: cyberspace." (2012: 2).

Joseph S. Nye Jr. points out that "There are dozens of definitions of cyberspace but generally "cyber" is a prefix standing for electronic and computer related activities." (Nye, 2010: 3). He seems to agree with Daniel T. Kuehl that cyberspace is "… an operational domain framed by use of electronics to …exploit information via interconnected systems and their associated infra structure." (Kuehl, 2009).

In comparison, United States' Department of Defense (DoD) provides the following definition of cyberspace: "Cyberspace is a global domain within the information environment. It consists of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Within cyberspace, electronics and the electromagnetic spectrum are used to store, modify, and exchange

data via networked systems. Cyberspace operations employ cyberspace capabilities primarily to achieve objectives in or through cyberspace." (The Department of Defense Joint Publication 3.0 Joint Operations, 22 March 2010).

All three definitions provide a brief insight into the technologies that cyberspace is built on and what cyberspace is used for. However, the Nye, Kuehl and DoD's definitions, respectively, go a step further than Reardon and Choucri by describing that cyber operations may achieve objectives in or through this virtual domain. This small difference in the definitions reflects the very significant fact that even though civilians have access to cyberspace and use it on a daily basis, the focus of a state institution is different and relates to security concerns; In other words, civilians emphasize the exchange of information as the more common use of cyberspace, while a state (represented by a state institution) focuses on how cyberspace may threaten the security of the state.

In academic literature, cyber *security* is also in focus, when defining cyberspace. Especially four features dominate the academic debate about what is often referred to as "the nature of cyberspace" (examples are Fischerkeller and Harknett, 2017 and Nye, 2017) and are essential to a discussion of states' motives and behavior.

First, low barriers to entry. The argument is, according to Nye (2010) as well as Fischerkeller and Harknett, (2017: 282), that compared to conventional power, which is based on economic and/or military resources, power in cyberspace is not as costly; Thus, without a vast amount of funding or a significant military capacity, in this domain a nation-state can still wreak havoc and skillfully seek to sway other nation-states through coercive digital means (Nye, 2010: 15). What is required in cyberspace is the knowledge of how to hack digital systems and even an economically backward state like North Korea or an internationally unpopular state like Iran have been able, with little resources, to acquire this knowledge.

Second, anonymity. According to Goutam (2015) and Fischerkeller and Harknett (2017), anonymity in cyberspace allows states to conduct shady cyber activities without fear of persecution, thus making some states bolder and inclined to cybercrime and/or destruction. Several researchers argue that in cyberspace, it is extremely difficult to prove who is behind cyber attacks (e.g. Goutam, 2015; Nye, 2017: 50). Although an attack can be traced to a particular IP address or otherwise be attributed to a specific hacker or hacker group, it is almost impossible to prove beyond all legal doubt a connection between such hackers and the states that sponsor them. This is referred to as the

Problem of Attribution in the academic literature and is often cited as a major problem when it comes to holding states accountable for their actions in cyberspace (e.g. Nye, 2017 and Shamsi et al., 2016). Since a connection to such attacks cannot be proved, it has become the rule rather than the exception that states deny their involvement in cyber attacks, even when all circumstances indicate the opposite (Fischerkeller and Harknett, 2017: 390). Even in cases, where the attacker, the state victim and the international community know beyond doubt that a state is behind an attack, it is at this point in time not possible to hold the attacker legally accountable, because there are no international regulation of state's conduct in cyberspace.

This leads to the third feature that is often described in relation to cyberspace: The lack of international laws or norms regarding state behavior. It took centuries of wars and two world wars to bring the international community together in signing international agreements that protect the sovereignty of states and thereby global peace. In comparison, cyberspace is a relatively new domain for state interactions and the entire palette of cyber attacks is likewise a new means of conducting war without conventional resources. Therefore, no international laws regarding cyberspace have been agreed upon yet. Accordingly, no legal tools are available yet, when dealing with a state that has violated the sovereignty of another nation-state in cyberspace. Some, like Wheeler (2018), argue that it is likewise too early to talk about cyber norms, while others, like Gomez (2018) advocate the emergence of norms in cyberspace.

The fourth feature of cyberspace is the lack of territorial delineation or a lack of an international definition of "sovereignty" in cyberspace. Just as there are no economic and legal barriers in this relatively new domain, conventional geographic barriers or limits do not apply in cyberspace. Some argue that in this virtual arena, the traditional definition of sovereignty, based on geographical borders, has no meaning. Therefore, it is not always easy to determine whether a cyber attack can be regarded as a violation of another state's sovereignty.

As mentioned above, several researchers argue that these four features (low barriers to entry; anonymity in cyberspace; the lack of international laws or norms; lack of an international definition of "sovereignty" in cyberspace) create new power opportunities for states who do not have conventional power in the form of military or economic resources, because they make it possible for such states to challenge the security of the world's superpower without the costs of conventional warfare. Thus, it becomes a warfare based on information rather than conventional weapons (Robertson and Arnold, 2018).

In this thesis, the brief definitions provided by Reardon and Choucri (2012), Daniel T. Kuehl and the DoD, respectively, are combined with the definition based on the four features above, thus leading to a definition of cyberspace that encompasses the physical technological devices whose connection point is the global "network of networks" as well as the electromagnetic spectrum itself (referred to as 'the virtual domain' going forward), where information is exchanged, modified and stored, and the above-mentioned four features.

2.3. Cyber conflict and cyber war (situations)

Due to a lack of common definitions and distinctions, the terms 'cyber conflict' and 'cyber war' seem to be used interchangeably and very casually in the academic literature as well as - and especially – in the media; thus, running the risk of misidentifying a lower-level cyber incident as a declaration of war.

It is especially important to distinguish between cyber conflict and outright cyber war, when examining the foundational claim of a Cyber Restraint Theory which emphasizes that there are different types of state behavior depending on the severity of the situation. Valeriano and Maness define cyber conflict as "… the use of computational technologies… in cyberspace for malevolent and/or destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities." (2015: 32). In addition, they describe the severity as "… a continuum where lower-level operations like [Distributed Denial of Service] incidents are the simplest forms of malice and higher infrastructure infiltrations are the most devastating and severe." (ibid.).

Likewise, Steiger, Harnisch, Zettl and Lohmann (2018) define cyber conflict as "… an incompatibility of stated intentions between actors which guides their use of computer technologies to harm the other…" In other words, it is characterized as disputes – political, economic or otherwise – that are carried out in cyberspace. Thus, according to both definitions, cyber conflict is a lower level of conflict than cyberwar and does not entail loss of lives.

In this thesis, a combination of Valeriano and Maness' (2015) and Steiger et al.'s (2018) definition is adopted. Accordingly, cyber conflict is considered disputes in cyberspace – through the use of cyber attacks – that may have material losses, but do not include attacks on infrastructure or lead to loss of lives.

While Valeriano and Maness do not provide an explicit definition of the term 'cyber war', they do describe conventional warfare as: "… destructive operations that seek to maim, kill, or wound physical individuals and/or to damage or destroy property.." (2015: 29) and explain that "for us, the prefix cyber simply means computer or digital interactions." (ibid., p. 22). In other words, cyber war is associated with the loss of lives. They, along with Lewis (2010), Gartzke (2013) and Rid (2012) argue that cyber war based on this definition has not yet and probably will not take place.

Other definitions of cyber war have also been suggested; Some like Joseph S. Nye Jr. focus on a definition based on the level of violence caused by operations in cyberspace (2011: 21). Others, like Seymour M. Hersh (2010), base their definition on the level of technological damage caused by cyber actions. Furthermore, Arquilla (2012) refers to another understanding of cyberwar as "… less a way to achieve a winning advantage in battle than a means of covertly attacking the enemy's homeland infrastructure without first having to defeat its land, sea, and air forces in the better part of a century…" This way of defining cyberwar implicitly puts emphasis on the swiftness of cyber operations, the possibility for the attacker of remaining hidden, and the lower costs of warfare in the virtual domain. In other words, it implicitly includes the first two features of cyberspace that were discussed above.

In this thesis, cyber war is defined as cyber actions that cause loss of lives or lead to severe technological damages to infrastructure, "… command and control structures of the military and foreign policy apparatus, wipe out the media communications of a state, destroy financial memory and wage economic combat, target the health industry and hospitals, or wither the ability of domestic units to protect the citizenry by eliminating technology used by police." (Valeriano and Maness, 2015: 40).

2.4. Cyber power and cyber weapons (how the entities deal with the situation)

The means of coercion and force in cyberspace differ from conventional means. In classic international relations (IR), military resources, economic and political means as well as social norms play a crucial role in the interactions between states, especially when it comes to swaying other states' political stances. Nye (2010: 3) argues that "power depends on context, and cyber power depends on the resources that characterize the domain of cyberspace." Thus, by this

definition, cyber power can be considered the array of different tools – in other words, cyber weapons used in cyber attacks – that the virtual domain provides.

Likewise, Ralph Langner defines cyberpower as "… a society's organized capability to leverage digital technology for surveillance, exploitation, subversion, and coercion in international conflict. A society wielding substantial cyber power can engage in a substantial number of actions: it can economically exploit or undermine other nations; gather political and military intelligence more efficiently than pre-digital espionage; interfere in foreign political discourse online; degrade an adversary's warfighting capabilities; sabotage critical infrastructure and industrial mass production, and even cause mass casualties." (Langner, 28 October 2016). Langner's definition resembles Nye's but is more elaborate in regards to defining what cyberpower can obtain.

Based on Nye's and Langner's definitions, in this thesis, cyber power is defined as the sum of a state's cyber capabilities. The different types of weapons, used in attacks (in this thesis, synonymous with the terms 'cyber incident' and 'cyber action') can be considered the power resources or the arsenal of weapons that nation-states have. Each of these types reflects a level of technological sophistication and thus gives an impression of the attacker's cyber capabilities.

Mainly six types of cyber weapons are discussed in the academic literature about cyber conflict: 1) Defacement/misinformation, 2) Disruption, 3) Infiltration, 4) Cyber terrorism, 5) Cyber crime, and 6) Espionage. The following definitions are the ones that have been adopted in this thesis.

Valeriano and Maness describe defacement/misinformation as "… website defacements or vandalism… This form of malice basically takes over the site for a few hours or days and displays text or pictures that demean or offend the victim site…" (p. 34).

Disruption through so-called Distributed Denial of Services (DDoS), are operations which "… flood particular Internet sites, servers, or routers with more requests for data than the site can respond to or process... This method shuts down the site, thereby preventing access or usage… Such methods are coordinated through *botnets*, or, more colorfully *zombies*, a network of computers that have been forced… to operate in the commands of remote users..." (ibid.)

Alford (2000) defines infiltration as "penetration of the defenses of a software-controlled system such that the system can be manipulated, assaulted, or raided." (p. 105). Infiltration is thus often the first step in a cyber attack.

According to Brickley (2012) cyber terrorism is "… the use of cyber capabilities to conduct enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change." This definition is, however, so broad that it encompasses most cyberattacks. Pope (2008) offers a narrower and more operational definition that is based on the intentions behind such an attack: "Unlike a nuisance virus or computer attack that results in a denial of service, a cyber-terrorist attack is designed to cause physical violence or extreme financial harm." (p. 1-2). A combination of these two definitions will be used in this thesis.

While Valeriano and Maness do not offer an explicit definition of cyberterrorism, they consider this type of cyber operations as "… the least a state can do with its toolbox of aggressive cyber actions" (2015: 50) and therefore not a violation of the cyber restraint norm that they believe governs state behavior in cyberspace.

Cyber crime is defined by Young and Yung (1996) as "… extortion-based attacks that cause loss of access to information, loss of confidentiality, and information leakage, tasks which cryptography typically prevents." This includes ransomware attacks, where the attacker demands ransom to liberate the hacked systems.

Finally, cyber espionage is, according to Valeriano and Maness, "… the use of dangerous and offensive intelligence measures to steal, corrupt, or erase information in… [cyberspace]" (2015: 49).

3. Theory

This Chapter contains a description of Cyber Restraint Theory, which is the main theory that this thesis focuses on in answering the research question. It also briefly introduces Friedrich Glasl's conflict escalation model, which is utilized to measure the concepts of 'severity' and 'impact' that Cyber Restraint Theory's claim builds on. An elaborate description of this model is provided in Chapter 4, where its stages are outlined and expectations regarding my three cases are specified.

3.1. Cyber Restraint Theory

In 2015, Brandon Valeriano and Ryan C. Maness presented a Cyber Restraint Theory in their book *Cyber War versus Cyber Realities*. In contrast to what they call the popular "cyber hype" (Valeriano and Maness, 2015: 28) regarding state interactions in cyberspace, they argue that A) almost all cyber incidents are between rivalries; B) that rivaling nation-states are governed by cyber restraint, and C) that low-level cyber attacks occur between rivals, are not subject to restraint because of their fairly harmless nature, and are in almost all cases motivated by regional conflicts over either territory or regime control (Valeriano and Maness, 2015: 66). Their point in focusing on rivals is that, if even the irrational players, who are most likely to resort to destructive cyber measures show restraint in cyberspace, then rational states will certainly do the same.

I have chosen Cyber Restraint Theory as the theory through which I seek to examine my research question: Is North Korean, Iranian and Saudi Arabian conduct in cyberspace characterized by restraint or do these states pose a threat to international peace? It was chosen due to its context-based approach; In the secretive digital domain, where attribution of attacks is difficult, Cyber Restraint Theory offers a solution in the form of looking at the political context to determine who an attacker is. It is an interesting angle, because it suggests that even though the domain has changed, states still behave as they have always done in the conventional domain of power struggles.

According to Valeriano and Maness, Cyber Restraint Theory is not based on a view of rivals as rational agents and does not concern itself with credible threats or perfect information (ibid., p. 56). Rather, it is based on social constructivism: "… the initial choice to launch a cyber operation and the response to offensive operations are socially constructed by the overall situation of rivalry and its history, the system of norms in operation at the time, and the nature of fear-based responses in

the attacked or threatened society." (2015: 51). Thus, an analysis of a cyber attack would have to focus on the social and political context in order to understand the motives of the attacker.

This is one of the strengths of this approach to cyber conflict, because political decisions are not made in a vacuum. As Thomas Risse puts it: "… human agents do not exist independently from their social environment and its collectively shared systems of meanings ("culture" in a broad sense)." (Risse, 2000: 5). It seems reasonable that political decisions should be based on cultural and historical stimuli as well as social and political interactions, the "social stories" created by politicians, the media etc. Dismissing this context or overlooking it would suggest that state behavior in cyberspace can simply be reduced to calculations of immediate gains and losses. To leap to such a conclusion would ignore the fact that even though cyberspace is a relatively new domain for state interactions or power plays, we are still dealing with the same players, who are still concerned about their security. The nation-states may have new power opportunities in cyberspace, but their foreign policy goals are overall the same, because they are not shaped by the domain in which they interact alone, but also by political history and culture.

In Cyber Restraint Theory, rivalries are defined as a pair of nation-states between whom "... there must be some degree of competitiveness, connection between issues, perception of the other as an enemy, and long-standing animosity..." (ibid., p. 52-53). Rivals are identified as the most likely entities to utilize offensive cyber weapons due to their long-standing relationship of hatred and competitiveness. Valeriano and Maness characterize such states as irrational in their behavior and argue that foreign policy decisions are "... often not made out of strategic rationality, but out of the simple, and perhaps immature, position of denying a gain to the enemy." (2015: 52).

They argue however that these rivalries are restrained in their choice of cyber weapons due to the fear of mainly five factors: 1) The possibility of the enemy replicating their attack and using it against them, 2) the interdependence of a globalized world means common interests and thus a fear of hurting one's own interests by attacking another state, 3) the fear of collateral damage, especially in the form of civilian costs, 4) the fear of conflict escalation beyond control, and 5) the fear of conventional economic or military retaliation (Valeriano and Maness, 2015: 62-64).

They stress that "[Cyber Restraint Theory] does not depend on… rational actors… only that the initiating side understands the drawbacks to its proposed action, and therefore will choose a more restrained approach to the situation." (2015: 56). Paradoxically, in order to expect rivals to weigh the gains of an attack against the mentioned risks and reach the conclusion that a restrained course

of action is preferable, they must possess some measure of rationality. If rivals are *not* rational, the five risk factors should not be expected to hinder cyber aggressions since counter-acting the enemy should be a higher priority. However, since Valeriano and Maness *do* argue that these risks restrain even rivals in cyberspace, some measure of rational behavior is assumed.

However, Valeriano and Maness emphasize that cyber restraint is not applicable to all levels of aggressions in cyberspace, only to majorly destructive cyber attacks, meaning "... direct and malicious incidents that might lead to the destruction of the energy infrastructure of a state, or incidents meant to take control of army units or facilities." (ibid., p. 62). These types of attacks are, according to Cyber Restraint Theory, generally avoided due to a fear of escalating the conflict beyond control and thereby leading to war as well as a fear of collateral damage and economic retaliation (ibid.).

Since minor cyber attacks are not subject to the same fear of escalation, they will and do occur because they "... do not require states to restrain themselves." (ibid., p. 59). Cyber Restraint Theory considers low-level incidents the tools that regional rivals use to signal displeasure or disagreement to each other (ibid., pp. 61-62), which means there should be no incidents of totally destructive attacks between rivals. This assumption is examined in this thesis by asking the question: Is North Korean, Iranian and Saudi Arabian conduct in cyberspace characterized by restraint or do these states pose a threat to international peace?

Valeriano and Maness present the following hypothesis about cyber restrained state conduct: "When cyber operations and incidents do occur, they will be of *minimal impact and severity* due to restraint dynamics." (2015:140).

The impact and severity of the chosen cyber attacks – the Sony Hack, Shamoon and the case of Jamal Khashoggi – will be measured by examining how far the conflict has escalated.

3.2. Friedrich Glasl's conflict escalation model

Friedrich Glasl presented his model of conflict escalation in his book *Konfliktmanagement. Ein Handbuch für Führungskräfte, Beraterinnen und Berater* in 1997. This model consists of nine stages that a conflict can escalate to, each stage more severe and reflecting a gradual decline from a civilized approach to more unscrupulous and primitive behavior.

In this thesis Glasl's stages will be used to determine the severity and impact of the thee cases of cyber attacks. These stages are described in detail in the following Chapter 4 and for each stage, it will be specified what the behavior of North Korea, Iran and Saudi Arabia will look like, if their respective cyber attacks reflect that specific stage of conflict.

4. Operationalization

To measure impact and severity of the Sony attack, Shamoon and the case of Jamal Khashoggi, respectively, three factors will be examined: 1) Rhetoric/behavior surrounding the cyber attack, 2) The aim of the attack, and 3) The impact of the cyber attack.

By examining the rhetoric/behavior surrounding the cyber attack, the intention is to find out two things. First, whether the attackers issued any warnings beforehand. One or more warnings would suggest that the cyber attack may have been considered a last resort by the attackers. Conversely, no warnings reflect an uncompromising attitude and thus that the attackers were intent on causing harm. Second, by looking into rhetoric/behavior surrounding the cyber attack, an understanding is gained of how the attackers, the victims and the media spoke of the attack – thereby examining whether the attackers made any announcements or demands that reflect their motives (and thus the severity of the conflict that is behind the attack), whether the state that a specific attack has been attributed to has denied its involvement, and whether the media has contributed to an escalation of the conflict. Thus, the announcements and actions of the parties involved in the cyber attack, will help determine the severity of the attack, and in turn whether the attack reflects cyber restraint.

By examining the aim of the attack, the intention is to understand what was specifically targeted. Such an understanding says something about the severity of the attack – for instance, there is a great difference between a cyber attack that only seeks to harass the victim and one that seeks to destroy the victim's power or even take one or more lives. Thus, the aim of the cyber attack will contribute to an understanding of the severity of the attack, and thereby whether the attack reflects cyber restraint.

By looking into the impact of the cyber attack, the intention is ultimately to find out whether the attack led to retaliatory measures - either in cyberspace or outside – and thus an escalation of the conflict. The material losses following the attack as well as its political impact will be examined. If

the conflict behind the cyber attack escalated after the hacking, it would suggest that the attack was so severe that it provoked a reaction. Conversely, if the conflict did not lead to retaliation, then there would be reason to consider Cyber Restraint Theory a plausible explanation. This way, the impact of the cyber attack will help determine the severity of the attack and ultimately whether the attack reflects cyber restraint.

4.1. Measurement of Severity and Impact of the cyber attacks

To measure the severity of rhetoric/behavior as well as the aim and impact of the Sony attack, the attack on Saudi Aramco and the case of Jamal Khashoggi, respectively, the level of devastation for each attack will be measured based on Friedrich Glasl's theory of conflict escalation.

Glasl argues that the escalation of a conflict is characterized by nine stages that each reflect a certain level of severity. To better understand the severity of each of the nine stages, they will be divided into three main levels of severity that each contain three distinctive stages.

The first level of the conflict escalation process – which can be described as 'Win-Win' situations – contains Glasl's first three stages ('Tension', 'Debate', and 'Actions'). This level relates to milder disputes in which both parties of the conflict may exit the conflict with a win in the form of a satisfying solution to the dispute.

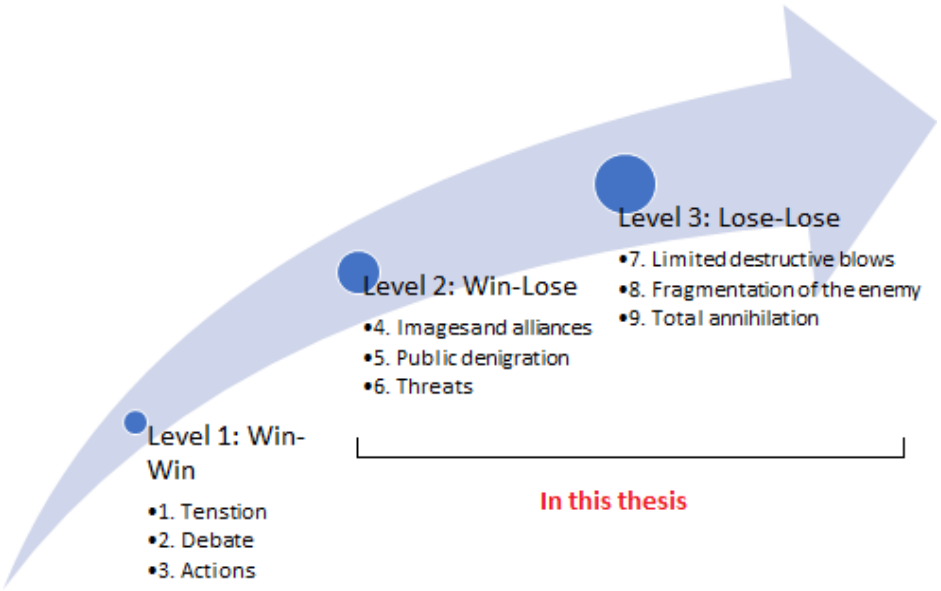
The second level – which is 'Win-Lose' situations – contains stages 4-6 ('Images and alliances', 'Loss of face' or 'public denigration' and 'Threats') and refers to a severity level on which at least one of the conflicting parties will suffer a loss in one form or the other.

The third and final level of conflict escalation is the destructive 'Lose-Lose' level, which contains stages 7-9 ('Limited destructive blows', 'Fragmentation of the enemy' and 'Total annihilation'), where neither of the conflicting parties gains anything from the conflict and thus their actions become about taking down the opponent rather than defending one's own interests.

Since level 2 represents situations, where it is still possible to reach a solution to the issue, its stages will be regarded as situations that are within the spectrum of cyber restraint. The dividing line between restrained behavior in cyberspace and unrestrained conduct is thus situations that have escalated from level 2 to level 3. This does not mean that conflicts on level 3 are automatically considered as non-restrained behavior, but rather they have reached a level, where restraint is no

longer a priority. The specific circumstances of the cyber attacks help determine whether it is indeed a case that reflects no restraint.

The figure below illustrates the three levels of conflict escalation and the three stages under each level:



Source: Own illustration, based on Friedrich Glasl's theory of conflict escalation and Jordan (2000).

Since the focus of this thesis is the conduct of states that are already in conflict with their opponent, it is possible to argue that my cases are beyond level 1 by virtue of the historic and long-lived animosity and hatred between them and their counterparts. Thus, only levels 2 and 3 are relevant for this thesis and only these two are included in the analysis.

In the following, stages 4-9 will be described and theoretical expectations relative to my cases will be outlined:

Stage 4: Images and coalitions (forming perceptions and alliances)

In this stage, the issue between the conflicting parties is "… no longer about concrete issues, but about victory or defeat." (Jordan, 2000: 3). In other words, it is no longer a friendly dispute to

which the parties are looking for a solution; The parties are becoming stubborn and fixed in their stances and seek to win rather than to find a solution.

The motivation behind the conflict becomes, at this stage, to gain an advantage in the power struggle with the adversary rather than to find a mutually beneficial solution. Neither party believes they are responsible for the escalation of the conflict because they consider their own actions as a response to the adversary's actions and intentions. (ibid.).

The conduct of the opposing parties is characterized by:

- *Portraying the counterpart as an enemy:* The very character of the opponent is perceived as the central issue in the conflict rather than irreconcilable political standpoints. Portraying the opponent as someone with "… certain characteristics (such as unreliability, incompetence, bossiness, etc.) only by virtue of belonging to [the other side of the conflict]." (ibid.).
- *Deniable punishment behavior:* "The counterpart is provoked, insulted and criticized, but in forms that do not formally infringe on the etiquette. Blows can be dealt through insinuations, ambiguous comments, irony and body language, but the perpetrator can flatly deny that any harm was intended, if challenged." (ibid, p. 4).
- *Attempts to affect the image of the opponent:* "Attacks are made on the identity, attitude, behavior, position and relationships of the counterpart." (ibid.).
- *Retaliatory actions:* "… since the other party cannot respond by openly discussing the incident, retaliatory action is very likely to ensue." (ibid.).
- *Forming alliances:* Each of the conflicting parties starts forming alliances with other states to strengthen their position.
- *No public scandals:* More or less latent deniable attacks "… [prevent] a dramatic public loss of face…" (ibid.), which is defined as public denigration. Stage 4 escalates to stage 5, when "… the basic honour of someone is offended repeatedly and deliberately, in particular in a public setting…" (ibid.).

For the Sony Attack, Shamoon, and the case of Jamal Khashoggi to be at stage 4 of the conflict escalation process, the following features would characterize North Korean, Iranian and Saudi Arabian cyber conduct, respectively:

- Portraying their adversary, rather than a specific dispute, as the issue of the conflict.
- Engaging in deniable punishment behavior.
- Attempting to affect the image of their opponent internationally.

- Conducting retaliatory attacks as well as being targeted by such attacks.
- Forming alliances with other states in cyberspace to strengthen their respective positions.
- No engagement in attacks that aim to humiliate their opponents publicly.

Stage 5: Loss of face (public denigration)

In this stage, the issue between the conflicting parties is "… no longer about concrete issues, but about the prevalence or not of holy values." (Jordan, 2000: 4). In other words, what was a specific disagreement at the beginning of the antagonistic relationship, e.g. about territory (stage 3) has escalated past an "us-against-them" fight in which the counterpart is defined as an enemy (stage 4), and has reached a stage (5), where the opponent is demonized and represented as "… destructive, subhuman, and bestial forces. The counterpart is no longer only annoying, but an incarnation of moral corruption." (ibid.).

The motivation for each of the parties is, at this stage, to gain a moral upper hand by protecting the forces of good (themselves) against the immoral forces of evil (the opponent). Stage 5 escalates to stage 6, when "… the parties start to issue ultimatums and strategical threats…" (ibid., p. 5).

The conduct of the opposing parties is characterized by:

- *Publicly denigrating the adversary*: "The [public] "face" [of the state] is hurt by public events, not by private [slander] or individual opinions." (ibid.).
- *A perception of compromise as humiliating:* "The gestures needed for establishing minimal trust in the sincerity of the other side become extreme and are often felt to be humiliating."
- *Retaliatory actions:* "Loss of face, and ensuing retaliatory acts often isolate the conflict parties from bystanders."

For the Sony Attack, Shamoon, and the case of Jamal Khashoggi to be at stage 5 of the conflict escalation process, the following features would characterize North Korean, Iranian and Saudi Arabian cyber conduct, respectively:

- Engaging in attacks that are publicly denigrating to the adversary state.
- Perceiving compromises as humiliating
- Conducting and are targeted by retaliatory attacks.

Stage 6: Threats

In this stage, the issue between the conflicting parties is about the fear of potential violence from the opponent and thus, "… the conflict parties resort to threats of damaging actions, in order to force the counterpart in the desired direction." (ibid.). In other words, the conflicting parties attempt to coerce the opponent to concessions by employing strategic threats.

The motivation behind each party's conduct is, at this stage, to prevent the adversary from using violence. Stage 6 escalates to stage 7, when "… the parties actively seek to harm the other side's sanction potential..." (ibid.).

The conduct of the opposing parties is characterized by:

- *Explicit threats of violent attacks on both sides*
- *Attempts at deterring the counterpart from attacking*

For the Sony Attack, Shamoon, and the case of Jamal Khashoggi to be at stage 6 of the conflict escalation process, the following features would characterize North Korean, Iranian and Saudi Arabian cyber conduct, respectively:

- Engaging in deterrence rhetoric.
- Issuing threats of violent attacks.

Stage 7: Limited destructive blows

In this stage, each party of the conflict "… expect[s] the counterpart to be capable of very destructive acts." (Jordan, 2000: 7). Thus, the characteristics of the relationship are mistrust, anger, fear and the lack of any constructive communication. Accordingly, "the parties see that it is no longer possible to win. It is a lose-lose struggle. Survival, and less damage than the counterpart suffers, are the main goals." (ibid.).

The motivation behind the conflict becomes, at this stage, to secure one's own survival by attacking the adversary's sources of power. Stage 7 escalates to stage 8, when "… attacks [are conducted] that are intended to shatter the enemy or destroy his vital systems." (ibid.).

The conduct of the opposing parties is characterized by:

Targeting the sanction-potential of the other: "… such as destroying or undermining the counterpart's financial resources, juridical status or control functions." (ibid.).

- *Less concern for ethical norms: "At earlier stages the parties exploited gaps in the norms, now they are cast aside if they are bothersome." (ibid.).*

For the Sony Attack, Shamoon, and the case of Jamal Khashoggi to be at stage 7 of the conflict escalation process, the following features would characterize North Korean, Iranian and Saudi Arabian cyber conduct, respectively:

- Conducting attacks that target their opponent's financial or juridical resources or their control functions.
- Showing no concern for ethical norms during the conflict.

Stage 8: Fragmentation of the enemy

In this stage, "… the attacks intensify and aim at destroying the vital systems and the basis of power of the adversary." (Jordan, 2000: 7).
The motivation behind the conflicting parties' behavior is to destroy the political systems that keep the opponent state coherent in order to secure one's own survival. Self-preservation, in fact, the only factor that restrains their conduct at this stage – no ethical or moral standards restricts the parties at this point, just like rational self-interest has been pushed to the background.

Stage 8 escalates to stage 9, when even self-preservation is no longer restricting their behavior.

The conduct of the opposing parties is thus characterized by:

- *Attacking the political coherence of the adversary to destabilize the opponent state internally:* "The system that keeps the counterpart coherent is attacked, hoping that the very identity of the other side will crumble so that it falls apart through its own internal contradictions and inherent centrifugal forces." (ibid).
- *Efforts to suppress domestic unrest:* The party that is threatened by internal destabilization takes strong measures to suppress domestic unrest.

- *Internal fragmentation:* The unity of the state disintegrates into smaller disagreeing factions; "Negotiators, representatives and leaders may be targeted, in order to destroy their legitimacy and power in their own camp." (ibid.).

For the Sony Attack, Shamoon, and the case of Jamal Khashoggi to be at stage 8 of the conflict escalation process, the following features would characterize North Korean, Iranian and Saudi Arabian cyber conduct, respectively:

- Attempting to destabilize their opponent internally.
- Taking strong measures to suppress domestic unrest.
- Suffering from domestic political fragmentation and conflicting factions.

Stage 9: Total annihilation

At the final stage of the conflict escalation process, even self-preservation is no longer a priority. Annihilating the enemy becomes paramount: "The only remaining concern in the race towards the abyss is to make sure that the enemy will fall too." (Jordan, 2000: 8).

The conduct of the opposing parties is characterized by:

- *The lack of concern for one's own survival*: At this stage, one may expect attacks that hurt both conflicting parties – such as suicide bombings or even nuclear bombings.

For the Sony Attack, Shamoon, and the case of Jamal Khashoggi to be at stage 9 of the conflict escalation process, the following features would characterize North Korean, Iranian and Saudi Arabian cyber conduct, respectively: Waging "a total war of destruction without scruples and remorse..." (ibid.) without any restrictions to the cyber weapons that may be used.

The table below is an overview of each conflict stage's strategic aim, motivation and methods as well as their respective escalation points, and the theoretical expectations regarding North Korea's, Iran's and Saudi Arabia's behavior, respectively:

	Strategic aim	Motivation	Methods	Escalation point to next stage	Theoretical expectation
Stage 4	Affecting the counterpart	Gaining the upper hand in the power struggle	Deniable punishment behavior	When the opposing parties repeatedly humiliate each other publicly	Deniable punishment behavior
Stage 5	Gaining a moral upper hand	The prevalence of values	Denigrating the other publicly	When ultimatums and strategical threats are issued	Public denigration of the adversary
Stage 6	Coercion	To block the counterpart politically	Threats of violence as a means of coercion	When the adversaries target each other's sanction potential	Threatening violent attacks
Stage 7	Neutralizing the other	Securing one's own survival	Targeting the sanction-potential of the other (financial, judicial resources)	When attacks occur that intend to shatter the enemy or destroy vital systems	Targeting financial resources and control systems
Stage 8	Destroying the basis of power of the other	To destroy the existence basis of the other	Vital systems are targeted	When self-preservation is given up	Attacking the political cohesion of the adversary to destabilize them internally
Stage 9	Total destruction	Total annihilation of the enemy, no self-perseverance instinct	Unrestricted war by any means and with any costs		War by all available means, even the mutually destructive

Source: Created based on Jordan (2000).

5. Ontological and epistemological assumptions

Ontology and epistemology, respectively, refer to the assumptions one makes about the world and how it is best understood. They are thus the foundation of my approach to the research question. Ontology and epistemology may, in other words, be respectively defined as "… the nature of reality (Hudson and Ozanne, 1988) and… the relationship between the researcher and the reality or how this reality is captured or known (Carson et al., 2001)." (Edirisingha, 2012). Thus, while ontology says something about how the world is, epistemology says how to understand or examine this world.

This thesis is built on the assumption of critical realism and thereby "… a transcendental realist ontology, an eclectic realist/interpretivist epistemology…" (Easton, 2010: 119). It is based on the belief that the world "… exists independently of our knowledge of it", but that it is also shaped by social interactions." (Sayer, 1992: 5). In other words, reality is not only based on perception – interactions between entities affect what the world looks like.

Implications for theory and methodology of this thesis

Basing my thesis on the position of critical realism has four important implications for my way of seeking to answer the research question.

First, an explanation of North Korean, Iranian and Saudi Arabian actions in cyberspace will be interpretivist. This is because it is based on data "… collected from people as well as from, and about, material things." (Easton, 2010: 124). As Sayer argues, "meaning has to be understood, it cannot be measured or counted, and hence there is always an interpretative or hermeneutic element in social science." (Sayer, 2000: 17). Thus, it is the study of "Social phenomena such as actions, texts and institutions, which may be interpreted in a variety of ways…" (Sayer, 1992: 5) – therefore, an understanding of the three states' behavior must be supported by a well-defined theoretical frame and a clear operationalization of the theory. Accordingly, Cyber Restraint Theory as well as Friedrich Glasl's conflict escalation model can be considered the lenses that the three states' actions are seen through. However, it is important to emphasize that according to critical realism, reality is not created by our perceptions. Even though it has "… to be interpreted by starting from the researcher's own frames of meaning, by and large [it] exist regardless of researchers' interpretation of [it]." (Sayer, 1992: 5).

Second, to understand whether North Korea, Iran and Saudi Arabia, respectively, show restraint in cyberspace, this thesis examines "… the external and visible behaviors of people, systems and things as they occur, or as they have happened." (Easton, 2010: 120). In other words, social and political interactions play a major role in understanding the three countries' conduct in cyberspace.

Third, the three selected states' actions cannot be explained independently of their political, historical and cultural context. Thus, the thesis is built on the perception that the attacking state's historical and political relationship as well as the two states' respective cultural backgrounds cannot be separated from an understanding of their behavior in cyberspace.

Fourth, critical realism works from the position that it is not possible to reach a definitive truth, when examining behavior. It is unlikely to reveal completely and lead to a full understanding of any social situation. Since there can be no definitive criteria to judge the "truth" of a particular version, critical realism relies on the researcher to collect further data that helps to distinguish among alternative explanations and on the community of researchers to debate them thoroughly." (Easton, 2010: 123). Specifically, this means that this thesis cannot reach an absolute and "correct" understanding of North Korean, Iranian and Saudi behavior in cyberspace – more research will always be needed in order to support what can be considered as temporary findings.

6. Methodology

In the following, the methodology of this thesis will be outlined. Thus, this chapter contains a description of research design, case selection, internal validity, reliability, replicability, external validity and sources.

6.1. Research design

This thesis is based on the methodological approach of process tracing, in which "histories, archival documents and interview transcripts… [are used] to see whether the causal process a theory hypothesizes or implies in a case is in fact evident in the sequence and values of … that case" (George and Bennett, 2005: 6).

I have furthermore chosen a deductive approach testing a subarea of deterrence theory, namely Cyber Restraint Theory, empirically through an examination of three cases: North Korean conduct in cyberspace, exemplified by the attack on Sony Pictures Entertainment of 2014; Iranian conduct in cyberspace, represented by the Shamoon attack in 2012; and Saudi Arabian behavior in cyberspace exemplified by the Khashoggi case of 2018.

Internal validity

A clear weakness in this research design is that - as with all studies of social events - it is impossible to take all explanatory factors, differences and similarities between the cases into account. In other words, studies of social phenomena cannot be controlled in the same way as experiments in a laboratory (Klotz and Prakash, 2006: 53). However, I have made an effort to counter this weakness by improving the quality of the data through internal validity, reliability, replicability and external validity (George and Bennett, 2005: 106).

Internal validity refers to the whether the used data supports that "x is the cause of the variation of y" (Yin, 2013: 47; Jackson, 2011: 24; Lawrence, 2007: 17). In other words, it is the cohesion of the research design – whether what one wishes to measure is actually measured. According to King, Keohane and Verba, "… it is easiest to maximize validity by adhering to the data and not allowing unobserved or unmeasurable concepts get in the way" (1994: 25). Thus, an effort has been made to describe the theoretical frame as clearly and as detailed as possible, provide a clear

operationalization as well as a comprehensive as possible outline of the methodology used in this thesis in order to make sure I measure what I wish to measure.

Reliability

A high reliability is when following the same conditions, a process consistently generates the same results (King et al., 1994: 25). In this thesis, reliability has been sought by applying the same methodology to three different cases.

Replicability

As mentioned, social phenomena do not work like laboratory experiments and just as it is difficult to take all possible explanatory factors into account, it is complicated to repeat a qualitative experiment. I have endeavored to counter this by providing an exhaustive bibliography to allow other researchers to examine the conclusions in this thesis (King et al., 1994: 26; George and Bennett, 2005: 106).

External validity

The findings in this thesis are not limited to the cases which are examined. In fact, this project aims to investigate the more "extreme" cases in order to be able to generalize the findings to states that do not have the same motivation for aggressive behavior in cyberspace. Thus, even though the focus is on North Korea, Iran and Saudi Arabia, the conclusions regarding their conduct in cyberspace contribute to an understanding of how states behave in general in the virtual domain. This supports external validity (Lawrence, 2007: 17; Goertz and Mahoney, 2012: 216).

6.2. Case selection

Overall, the cases examined in this thesis are chosen based on the logic that economically or politically desperate states are less likely to exercise self-control rather than display aggressive behavior. Particular emphasis has been placed on international status, economic situation and regional conflicts in the choice of cases. The idea behind the choice of states most likely to choose an aggressive strategy is that, if even these states demonstrate self-restraint in cyberspace, then Cyber Restraint Theory is very likely to be applicable to other, less desperate, states.

Specifically, North Korea, Iran and Saudi Arabia have been selected as the cases in this thesis due to three factors that might motivate them to seek power in order to enhance their position. By focusing on states that are strongly motivated to seek influence, one should be able to test the validity of Cyber Restraint Theory; In other words, if even states who see a strong reason to seek power restrain themselves in cyberspace, then Cyber Restraint Theory is a plausible theory of state behavior in cyberspace.

The first factor behind the selection of North Korea, Iran and Saudi Arabia is their respective international statuses as controversial states. North Korea and Iran have traditionally been regarded as rogue states, because of their pursuit of nuclear weapons. Financial sanctions have been imposed on them because of their conduct, and they are usually spoken of as unruly and irrational states. It is useful to examine whether Cyber Restraint Theory applies to politically shunned states, who might be desperate to gain power in order to enhance their position.

While Saudi Arabia has not traditionally been regarded as a rogue state by the international system, it has been seen as highly controversial due to its non-democratic domestic affairs; It is perceived as an ally of the West, but a contradictory relationship remains with the Western world due to political and social values that are at odds with liberal democratic values. Saudi Arabia has thus been included in this thesis as a state, which is 'between two worlds".

The second factor behind the selection of North Korea, Iran and Saudi Arabia is their distinctive economic situation. Since North Korea and Iran are regarded as rogue states, economic sanctions have been imposed on them as a coercive measure in an attempt to deter them from their current political path of developing nuclear weapons. These sanctions weigh heavily on North Korea's and Iran's economy, respectively, and might motivate them to take aggressive measures in cyberspace as a means of asymmetrical warfare. If even states that are in bad shape economically restrain themselves in cyberspace even though cyber operations may provide power, then Cyber Restraint Theory must be valid. In this respect also, Saudi Arabia stands out. Economically (and therefore also regarding political influence), the prosperous Saudi Arabia is in a power situation compared to North Korea and Iran, who are pressured economically because of the internationally imposed sanctions. Again, Saudi Arabia has been included as a case in which conditions are different compared to North Korea and Iran in order to test the scope of Cyber Restraint Theory; In other words, it is to see whether the theory is limited to states, who may have a desperate need for power to survive. If Saudi Arabia shows restraint in cyberspace, it might indicate that it is not the case.

The third factor behind the selection of North Korea, Iran and Saudi Arabia is that the three cases are all part of on-going regional conflicts in which they have a local/regional rival that is perceived as a threat to their national security. North Korea's rival is South Korea that has allied itself with the United States. In Iran's case, Saudi Arabia is the rival and also an ally of the United States. Finally, Saudi Arabia's main rival is Iran, whose alliances are with Saudi Arabia's neighbor, Qatar, as well as Russia and China.

Regional conflicts are usually either about territorial disputes (Vasquez and Leskiw, 2001) or "one state might target another with cyber operations in order to remove and discredit the leader in charge." (Valeriano and Maness, 2015: 66). In the specific case of North Korea, the years-long dispute with South Korea is connected to a territorial dispute, while the animosity between Iran and Saudi Arabia is rooted in a religious quarrel between Shia and Sunni Muslims, which is fought through proxy battles in an attempt to overthrow the respective governments by destabilizing the region.

Valeriano and Maness argue that rivalries are the most likely entities to engage in cyber conflicts because of a long-standing animosity and because "foreign policy perspectives during a rivalry are often not made out of strategic rationality, but out of the simple, and perhaps immature, position of denying a gain to the enemy." (2015: 52). If even the conduct of rivals in cyberspace is characterized by restraint, then the theory of cyber restraint should apply to other states in cyberspace.

In sum, the selected cases represent entities that are in an economically or politically frustrating situation and are thus likely to pursue an aggressive cyber policy. However, if these states display restraint in cyberspace, then Cyber Restraint Theory is a plausible theory of state interactions in the virtual domain.

Selection of cyber attacks

For each of the three cases, a cyber attack that has been attributed to them has been selected as an example of their conduct in cyberspace. In North Korea's case, the attack on Sony Pictures Entertainment was chosen; in Iran's case it was the Shamoon virus; and in Saudi Arabia's case, the selected cyber attack was the case of Jamal Khashoggi. The choice of cyber attacks that exemplify each of the three states' conduct in cyberspace is based on three factors. The first reason behind the selection of these attacks is that there are strong indications that each of them was politically

motivated – a retaliation in cyberspace for a specific political issue. As mentioned, political disputes, especially between rivals, tend to take on a ruthless and savage character that is more prone to escalation (ibid.). In choosing attacks that occur amid political tensions between the attacker and the victim, I seek to draw conclusions based on a setting – a political context – in which the respective attackers would be more likely to resort to escalatory tactics rather than restraint. If such cyber attacks reflect a measure of restraint – despite the popular hype – it would support the hypothesis of Cyber Restraint Theory.

Second, these specific cyber attacks were chosen because they are examples of different cyber weapons. While the Sony Hack was a combination of a ransomware attack and disruption, the Shamoon virus was an example of infiltration, and the case of Jamal Khashoggi one of surveillance. Since different cyber weapons reflect different capabilities (levels of sophistication), I seek to test whether Cyber Restraint Theory holds true for both highly capable states as well as states with limited cyber capabilities.

Third, these specific cyber attacks were chosen because they are examples of attacks on different targets; Sony is a privately-owned company, Saudi Aramco is a state-owned company and in the case of Jamal Khashoggi, the target was an individual. By including cyber attacks on different types of targets, the aim is to test whether nation states' cyber actions are restrained no matter the kind of target that is in question.

In sum, the respective cyber attacks, which were chosen to exemplify North Korean, Iranian and Saudi Arabian conduct in cyberspace, were selected due to their political character and their differences with regard to cyber weapons and target types. If cyber restraint is evident in all three cases, it would indicate that Cyber Restraint Theory is a plausible explanation. If, however, one or more of the cases do not reflect cyber restraint, it would be considered a challenge to the theory.

In choosing controversial states in cyberspace, the obvious choice may have been China and Russia seeing as they are significant adversaries to the West in cyberspace and allegedly have the cyber capabilities to cause serious harm to international peace (Breene, 2016). However, much focus is already on assessing the danger that China and Russia pose and in comparison, less attention is paid to North Korea, Iran and Saudi-Arabia - often because their cyber capabilities have been underestimated due to an assumed general technological or economic backwardness, or in Saudi Arabia's case, because it is considered an ally of the West. However, cyber attacks like the attack on Sony Pictures Entertainment in 2014, the Shamoon virus that hit Saudi Aramco in 2012 and the

case of Jamal Khashoggi in 2018 have proven that the three countries hold the potential of causing serious harm in and beyond cyberspace. Accordingly, I find that assessing the threat from previously underestimated or overlooked players is highly relevant.

6.3. Limitations

As mentioned, cyber conflict is a relatively new field in International Relations, and therefore the development of theories about the virtual domain and its consequences is also in its infancy. This means that even though there currently is not shortage of examples of cyber attacks or media coverage of such attacks, an academic understanding of state behavior in cyberspace is still evolving. In relation to my choice of topic and the focus of this thesis, it has meant that I have chosen to focus on a theory that has presented an explanation of state dynamics in cyberspace, and chosen to examine whether its underlying hypothesis holds, when it is empirically tested.

Finally, it has not been my intention to cover all aspects of Cyber Restraint Theory, the three cases' cyber activities or the overall dynamics of cyber conflict - only to the extent that it answers the research question of this thesis. Thus, this thesis focuses narrowly on empirically testing Cyber Restraint Theory's underlying hypothesis or assumption that all cyber incidents will be of limited severity and impact because states restrain themselves in cyberspace due to fears of conflict escalation.

6.4. Sources

The sources that have been used in my project are divided into three areas of application: 1) To outline the two theories that have been utilized, 2) To describe the general conduct of North Korea, Iran and Saudi Arabia in cyberspace, and 3) To provide the analyses with evidentiary support.

Outlining the two theories that have been used in this thesis:

Valeriano and Maness (2015) have been utilized to develop the research question of this thesis and to outline Cyber Restraint Theory.

Jordan (2000) has been used to outline Friedrich Glasl's conflict escalation model, which has been selected as the measure of the cyber attacks' severity and impact. The optimal strategy would have been to use a firsthand source, namely Glasl's book *Konfliktmanagement. Ein Handbuch für*

Führungskräfte, Beraterinnen und Berater, where the theory was first presented in 1997. However, since it was published in German, because of the language barrier, Jordan (2000) has been used in this thesis. His description of Glasl's nine stage escalation model "… has been scrutinized and approved of (with some corrections) by Friedrich Glasl." (Jordan, 2000). Thus, even though Glasl's book has not been cited in this thesis as the source, Jordan's description of the theory has been approved by Glasl himself and is therefore an optimal alternative in this case.

Data sources used to describe the three states' general conduct in cyberspace and used in the analyses:

Where it was possible, I have sought first-hand accounts - e.g. by looking up information about United Nations responses on The United Nations' own website, info about government responses in the respective government sources and by using the cyber attackers' original messages, where possible.

However, in many cases, it was not possible to find information via such sources. As an example, no account about the cyber attack in 2012 was to be found on Saudi Aramco's website. Likewise, firsthand data about North Korea's reaction to the Sony Hack as well as firsthand accounts of Iran's reaction to the cyber attack on Saudi Aramco are scarce. Even if it was possible to find such specific accounts, there would still be a linguistic barrier, since I do not read neither Korean nor Persian. Therefore, mainly news articles have been utilized in such cases. Since most cyber incidents have a covert element, information of cyber attacks is often based on secondhand information.

News outlets have been used to outline widely known facts that can be found in other news outlets and academic literature of the time. The possibility of underlying interests or positions that may affect the information have been countered by looking up the events of the three cyber attacks in several sources. In other words, since media outlets can have a certain sensational perspective, I have sought to enhance the trustworthiness of information, collected from these sources, by confirming the validity of the information in two or three other sources.

Finally, academic sources like Nye (2010, 2011 and 2017), Fischerkeller and Harknett (2017), Sullivan (2016), Gomez (2018), Arquilla (2012) and others, were used to outline the broad lines of the academic debate on cyberspace and cyber conflict as well as further support the arguments presented in the analyses.

7. Brief overview of the general conduct of North Korea, Iran and Saudi Arabia, respectively, in cyberspace

The following are brief descriptions of the general conduct of North Korea, Iran and Saudi Arabia, respectively, in cyberspace. Each description addresses the respective state's aims in cyberspace, the overall impact of its cyber actions as well as the overall severity of its cyber actions by relating them to Glasl's conflict escalation model.

7.1. North Korea

North Korea is heavily sanctioned by the international community for its pursuit of Weapons of Mass Destruction (Albert, 2019) and seems to have grown gradually more desperate, both economically and politically.

North Korea's actions in cyberspace have been described as "a wave of cybercrime" (Shubber and Sevastopulo, 2018). The country's conduct in the virtual domain is associated with theft and extortion – and mainly ransomware attacks. These attacks are, according to the United Nations, a way to circumvent the economic sanctions that have been placed on the country by the international community (De Luce and Mitchell, 2019).

Aims in cyberspace

Some of the largest cyber attacks that have been attributed to North Korea are the Sony Hack in November 2014, the Bangladesh cyber bank heist in February 2016, and the WannaCry attack in May 2017. The first and the last are examples of ransomware attacks, where information or computer networks were leveraged for funds. The Sony Hack developed into a politically motivated attack, however, but this is elaborated on and analyzed further in the analysis section. In the Bangladesh cyber bank heist, SWIFT accounts (SWIFT is the international communication platform for banks) were taken over to send "… more than three dozen fraudulent money transfer requests to the Federal Reserve Bank of New York asking the bank to transfer millions of the Bangladesh Bank's funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia." (Zetter, 2016). All three are thus examples of cyber crime, where different entities were targeted by means of extortion or theft in order to coerce or trick money out of them.

Overall impact of cyber actions

In the Sony Hack a privately-owned company, located in the United States, was targeted. The attack caused both economic and reputational losses but lead to no technological or physical destruction. In the Bangladesh Bank heist, one bank was the target and the cyber attack led to the theft of millions (ibid), but likewise, this attack caused no technological or physical devastation. The WannaCry attack, however, affected 150 countries (BBC, 19 December 2017), including "… hospitals, telecommunications firms and other companies…" (CBS News, 12 May 2017). Although the cyber attack led to wide-spread and potentially dangerous consequences by affecting, among other things, hospitals, the motive behind it seems to have been collecting money through extortion rather than physical devastation. Furthermore, even though the attack caused much panic, especially in hospitals, it did in fact not lead to known losses of lives.

Overall level of severity of cyber actions

Relating North Korea's actions in cyberspace to Glasl's nine stages of conflict escalation, it can thus be argued that since its efforts in the virtual domain have mainly been focused on cyber crime, and thus extortion and theft – rather than destruction – North Korean conduct is not consistent with the most severe level (level 3). Rather, it seems to fit level 2 of Glasl's conflict escalation spectrum, where the impact of attacks is limited.

7.2. Iran

Iran is, like North Korea, heavily sanctioned by the international community due to its pursuit of Weapons of Mass Destruction (Sanger et al., 2019**).** Nevertheless, the Iranian regime has continued its efforts – even after a devastating cyber attack in 2010 – the Stuxnet worm – which targeted Iran's nuclear program (Langner, November 2013). Furthermore, Iran has defended its position by targeting its adversaries' sanction-potential – namely, their sources of international influence.

Iran has been "… described by one European intelligence chief as being a major cyber threat to the West, third only in its behavior to Russia and China." (Bunkall, 2019). Furthermore, as a state which is "… engaged in an ongoing cyber campaign against the West…" (ibid.).

Several cyber espionage and disruption attacks against Western countries as well as Iran's regional rival, Saudi Arabia, have been attributed to the Iranian regime, including "… breaches and fake

social media activity" (Doffman, 2019) as well as "… aggravated access to computer systems, wire fraud and stealing proprietary data." (Bunkall, 2019).

Aims in cyberspace

Iran is part of a regional conflict with Saudi Arabia. The conflict can be said, at its core, to be one of religious ideologies, since it is a continuous fight between Shia Muslims in Iran and Sunni Muslims in Saudi Arabia. This conflict has manifested in proxy battles in the region (Marcus, 2017), and it can be argued that the same conflict is motivating Iran's conduct in cyberspace.

Iran's behavior in the virtual domain is characterized by attacks, which target the sanction-potential of its adversaries – in other words, the main targets are its opponents' sources of power. This has been described as "… cyber-enabled economic warfare – a strategy involving cyber attacks against an adversary's economic assets in order to reduce its political and military power." (Fixler and Cilluffo, 2018: 6).

The cyber attack on the state-owned company Saudi Aramco, which has been attributed to Iran, targeted an oil company in a country, where a great part of its GDP builds on its export of oil (Export.gov, 11 May 2018). Saudi Arabia's influence on the international scene is also rooted in its oil export, since Saudi Aramco is the world's largest supplier of oil (Olson, 2012).

Thus, Iran's primary aim in cyberspace seems to be targeting its adversaries' sanction-potential in order to ensure the regime's survival.

Overall impact of cyber actions

The U.S intelligence community has determined the impact of Iranian conduct in cyberspace to be "… capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks..." (Coats, 2019: 6). In other words, although Iranian cyber capabilities are developing rapidly **(**Fixler, 2019), at this stage, they are still of limited impact.

Overall severity of cyber actions

Relating Iran's actions in cyberspace to Glasl's nine stages of conflict escalation, it is thus possible to argue that since its efforts in the virtual domain have mainly been focused on targeting the power sources of its opponents in order to secure the Iranian regime's survival , Iranian conduct is not

consistent with the milder level 2. Rather, it seems to fit level 3 of Glasl's conflict escalation spectrum, which is the highest level of severity and impact.

7.3. Saudi Arabia

Saudi Arabia is a relatively new player in cyber conflict. The kingdom has been the target of several cyber attacks, but its capabilities are still developing, and it does not seem to primarily focus its efforts on international conflict in the virtual domain. Rather, cyber weapons are used to maintain control of its own population to prevent political unrest.

In authoritarian regimes, where power is focused in the hands of either a religious or political elite, the influx and exchange of information via cyberspace is one of the greatest challenges to the government's power (Hirst, 2012). The empowerment of the population, through the exchange of information and ideas, is often seen as the biggest threat to the government (ibid.). Therefore, the most important aims in cyberspace become controlling this communication, before it sparks political unrest.

Most of the revolutions in the Arab region that are now collectively called the Arab Spring began on social media and led to the populations toppling their respective governments (Dewey et al., 2012).

Aims in cyberspace

The Saudi monarchy survived the Arab Spring, but seems to be continuously monitoring social media, where troll farms verbally attack and intimidate anyone, who attempts to criticize the regime (Benner et al., 2018). Troll farms are "…organization[s] set up in order to publish a large number of messages or posts on the internet, that often appear to be from people who do not really exist, and that are intended to cause trouble, influence political views, etc." (Cambridge Dictionary).

In some cases, like the case of the Saudi activist Jamal Khashoggi, cyber surveillance has facilitated physical assaults or led to arrests (Freedom on The Net 2018, Saudi Arabia).

Thus, Saudi Arabia's primary aim in cyberspace seems to be cyber surveillance of its own population in order to ensure the survival of the Saudi regime.

Overall impact of cyber actions

Internationally, Saudi Arabia's cyber presence may be modest at this point in time, but domestically, its cyber surveillance has massive costs in the form of human rights violations (Human Rights Watch, World Report 2019). Social media is monitored for political opposition and oppositionists are punished either virtually or physically for their utterings (Freedom on the Net 2018, Saudi Arabia). The case of Jamal Khashoggi, which is analyzed in Chapter 7, illustrates the level of severity and impact of the Saudi regime's actions in cyberspace.

Overall severity of cyber actions

Relating Saudi Arabia's actions in cyberspace to Glasl's nine stages of conflict escalation, it can thus be argued that since its efforts in the virtual domain have mainly been focused on cyber surveillance with the aim of suppressing political opposition, Saudi conduct is not consistent with the milder level 2. Rather, it seems to fit level 3 of Glasl's conflict escalation spectrum, which is the highest level of severity and impact.

The following Chapter 8 contains an analysis of North Korea, Iran and Saudi Arabia, respectively. Each analysis focuses on a cyber attack that exemplifies the respective state's conduct in cyberspace. The cyber attack is analyzed using Glasl's conflict escalation model in order to determine, if the attack was of limited severity and impact as Cyber Restraint Theory claims. In turn, it is determined, whether North Korean, Iranian, and Saudi Arabian conduct in cyberspace is characterized by cyber restraint.

8. Analysis: Is North Korean, Iranian and Saudi Arabian conduct in cyberspace characterized by restraint or do these states pose a threat to international peace?

Chapter 8 is divided into three analyses: 1) North Korea's behavior in cyberspace: The Sony Hack; 2) Iran's behavior in cyberspace: The cyber attack on Saudi Aramco; and 3) Saudi Arabia's behavior in cyberspace: The case of Jamal Khashoggi – thus, one for each of the cases that were selected in this thesis.

In each analysis a timeline of the cyber attack is provided, followed by an examination of the attack's severity and impact. The severity is determined by examining the rhetoric and behavior of the conflicting parties surrounding the cyber attack as well as the aim of the attack.

The impact is examined in terms of material losses and political escalation of the conflict. However, it is primarily the political escalation following the attack that is the focus in determining the impact of the attack since an escalation may lead to more destructive interactions in cyberspace (thereby escalating to a new stage of Glasl's conflict escalation spectrum). What is ultimately looked at by analyzing the severity and impact is whether the cyber attack reflects a restrained behavior in the virtual domain.

An interim conclusion follows for each analysis section of whether the cyber attack was of limited impact and severity as Cyber Restraint Theory claims.

Finally, each analysis is rounded by a discussion of whether the selected cyber attack is representative of the respective state's general conduct in cyberspace and if this overall behavior reflects cyber restraint. Each analysis section's discussion is intended as a starting point for a more comprehensive discussion in chapter 7 of whether North Korean, Iranian and Saudi conduct in cyberspace is characterized by restraint or these states pose a threat to international peace.

8.1. North Korea's behavior in cyberspace: The Sony Hack

In November 2014, Sony Pictures Entertainment ('SPE' or 'Sony' going forward) was hit by a cyber attack which may be described as a ransomware attack that developed into politically motivated extortion. Sensitive information about Sony employees, internal emails and company secrets were leaked online in an attempt to prevent Sony from releasing the movie *The Interview.*

The attack on Sony is widely attributed to North Korea "who expressed outrage over the Sony-backed film "The Interview," an action-comedy centered on an assassination plot against North Korean leader Kim Jong Un." (Peterson, 2014). Thus, the political context of the cyber attack on SPE in 2014 suggests that North Korea was the most likely attacker.

To assess the severity and impact of the cyber attack – and thereby the validity of Cyber Restraint Theory – the following chapter will provide A) a timeline of the attack followed by B) an analysis of the rhetoric and behavior during the attack as well as the aim and the impact of the cyber attack on SPE based on Glasl's conflict escalation model; C) an interim conclusion of the severity and impact of the Sony Hack; and finally, D) a discussion that compares the cyber attack with North Korea's general conduct in cyberspace and discusses whether such behavior reflects restraint in cyberspace.

8.1.1. Timeline of the cyber attack on Sony Pictures Entertainment

To understand the severity and impact of the cyber attack on SPE, it is important to provide an overview of the events that unfolded during the attack.

The following is a timeline of the attack on SPE in November 2014:

- *Phase 1: Attempts at a political resolution through official channels*
  On June 11, 2014, UN Secretary-General Ban Ki-Moon received a letter from North Korea, complaining that the Sony produced movie *The Interview* (which is a comedy revolving around an assassination attempt on North Korean leader Kim Jong-un), was an "undisguised sponsoring of terrorism, as well as an act of war." (United Nations General Assembly Security Council, 27 June 2014). The North Korean ambassador also attempted to appeal to the United Nations, requesting that the Security Council would condemn the movie, but the UN Council did not consider it an urgent matter of security (Holm, 2017: 24).

- *Phase 2: Threats of hacking Sony - A ransom was demanded*

  On November 21, 2014, *Sony executives Michael Lynton and Amy Pascal received ransom emails from "God'sApstls" demanding money in exchange for refraining "...*from compromising the security of the company's computer systems..." (Holm, 2017: 24). The emails stated: "[W]e've got great damage by Sony Pictures. The compensation for it, monetary compensation we want. Pay the damage, or Sony Pictures will be bombarded as a whole. You know us very well. We never wait long. You'd better behave wisely." (Sullivan, 2016: 439).

- *Phase 3: Threats of releasing company secrets unless demands were met*

  On November 24, 2014, Sony was hacked by a group identifying themselves as "Guardians of Peace" (GOP). An image of a skull appeared on the computer screens of Sony employees along with the message: "This is just the beginning... [W]e've obtained all your internal data." (Sullivan, 2016: 439). The hacker group threatened to release company secrets unless Sony obeyed their demands (Holm, 2017: 24-25; Sullivan, 2016: 439). The GOP was subsequently linked to the North Korean government by the FBI (Holm, 2017: 24-25).

- *Phase 4: The GOP draws the media's attention to Sony leaks*

  On November 29, 2014, *The GOP informed the media of Sony leaks*: "… Kevin Roose, a senior editor at Fusion.net, was one of several journalists who received an email stating: "Hi, I am the boss of G.O.P. A few days ago, we told you the fact that we had released Sony Pictures films including Annie, Fury and Still Alice to the web. Those can be easily obtained through internet search. For this time, we are about to release Sony Pictures data to the web. The volume of the data is under 100 Terabytes." (Sullivan, 2016: 439; Seal, 2015).

- *Phase 5: Threats of physical harm to Sony employees and their families*

  On December 5, 2014: Sony employees received emails in which the GOP threated their and their families' safety unless they signed a denunciation of Sony (Holm, 2017: 25).
  The message was: "Many things beyond imagination will happen at many places of the world. Our agents find themselves act in necessary places. Please sign your name to object the false of the company at the email address below if you don't want to suffer damage. If

you don't, not only you but your family will be in danger." (Sullivan, 2016: 440).

- Phase 6: *North Korea denies involvement*
  On December 7, 2014, North Korea officially denied involvement in the attack on Sony but described it as a "righteous deed." (Sullivan, 2016: 440).

- *Phase 7: Threats of war by the GOP*
  On December 8, 2014, further threats were issued by the GOP, this time threatening a war: "[S]top immediately showing the movie of terrorism which can break regional peace and cause the War!" (Sullivan, 2016: 440).

- *Phase 8: Further threats of war by the GOP*
  On December 16, 2014, The GOP demanded that the Sony produced movie *The Interview* not be released and threatened war, if Sony decided to release it (Sullivan, 2016). As Holm (2017: 26) and Robb (2014) point out, this was the first time *The Interview* was mentioned during the attack on Sony.

- *Phase 9: Sony decided to stop the release of The Interview*
  On December 17, 2014, Sony decided to not release *The Interview* (Holm, 2017: 26).

- *Phase 10: Sony revoked the decision to stop the release of the Interview*
  On December 23, 2014, Sony revoked the decision to stop the release of *The Interview* (Pomerantz, 2014).

8.1.2. Analysis: Severity and impact of the cyber attack

In order to determine the severity and impact of the cyber attack on Sony Pictures Entertainment, the course of events before, during and after the attack will be examined and compared to Glasl's conflict escalation model. Specifically, the rhetoric and behavior surrounding the conflict will be examined, the aim of the cyber attack as well as its impact. By determining which stage of conflict the attack belongs to, it will be possible to determine whether it was of limited severity and impact as Cyber Restraint Theory claims.

Rhetoric and behavior

In order to determine the severity of the cyber attack on Sony, the rhetoric surrounding the cyber attack, as well as the behavior of the conflicting parties will be examined. Using the process of elimination, it is possible to argue that level 3 of Glasl's conflict escalation model (the so-called "Lose-Lose"), and thus stages 7-9, is too destructive to describe the cyber attack on Sony. Level 3 is characterized by the fact that the conflicting parties no longer regard the issue as something that can be solved and perceive each other as a threat that undoubtedly threatens their own survival. At this level, the conflict no longer revolves around a concrete and delimited issue, but about the parties' survival. The level 3 attack targets are respectively the opponent's sanction potential (stage 7), political systems that support the opponent's political cohesion (stage 8) and the opponent's survival (9). The cyber attack on Sony is below this level of escalation, seeing as the alleged reason for the attack was a specific issue – the Sony produced move *The Interview* – and the target of the attack was limited to one company.

Likewise, stages 5 and 6 are characterized by a rhetoric, a behavioral pattern, an aim and impact that cannot be found in the course of events surrounding the cyber attack on Sony. Rather, a number of factors indicate that the attack is a stage 4 conflict according to Glasl's escalation model.

First of all, the primary characteristic of a stage 4 conflict is so-called '*deniable punishment behavior':* "The counterpart is provoked, insulted and criticized, but in forms that do not formally infringe on the etiquette… the perpetrator can flatly deny that any harm was intended, if challenged." (Jordan, 2000: 4). Thus, officially no specific attack can be attributed the conflicting parties, but it is clear that there is a conflict.

In the specific context of the attack on Sony, the North Korean government officially distanced itself from the attack even though the FBI later believed that evidence was found of North Korean involvement (FBI National Press Release, 19 December 2014). Likewise, the timing of the attack on Sony, which came after the North Korean government sent a letter to UN General-Secretary Ban Ki-Moon regarding the Sony produced movie *The Interview*, seems suspicious seeing as the GOP demanded that Sony should halt the release of the film. These factors indicate that a type of attack was employed that allowed North Korea to stay in the shadows and as mentioned in section 2.2. of this thesis, cyberspace is a domain in which direct attribution can be complicated. Choosing such a course of behavior is thus in accordance with stage 4 of Glasl's conflict escalation model.

Furthermore, in stage four, neither party believes they are responsible for the escalation. They consider "… their behavior… a reaction to the counterpart's actions and intentions…" (Jordan, 2000: 3). North Korea explicitly referred to releasing *The Interview* as a terrorist act, as an action that would escalate the issue to the point of war and warned about it beforehand and while it denied any involvement in the cyber attack on Sony, it described the attack as a "righteous deed", which indicates that North Korea sees the escalation of the issue as a consequence of Sony's – and perhaps the UN's – lack of action regarding stopping the release of *The Interview* rather than as an immoral assault on Sony. This perception of the conflict is also in accordance with Glasl's stage 4 of conflict escalation.

According to the characteristics of Glasl's stage 4 of conflict escalation, the opponent is at this stage referred to as someone whose stance in the conflict says something about his character. The very character of the opponent is perceived as the central issue in the conflict rather than irreconcilable political standpoints. The opponent is portrayed as someone with "… certain characteristics (such as unreliability, incompetence, bossiness, etc.) only by virtue of belonging to [the other side of the conflict]." (Jordan, 2000: 3). On June 11th, 2014, North Korea attempted to appeal to UN Secretary-General Ban Ki-Moon through a letter, complaining that the Sony produced movie *The Interview* was an "undisguised sponsoring of terrorism, as well as an act of war." (Security Council Report, A/68/934–S/2014/451). It is thus possible to argue that the UN as well as Sony are considered accomplices to terrorism by the North Korean government for refusing to halt the release of *The Interview.* This view of the opponent is therefore in accordance with stage 4 of Glasl's conflict escalation model. Jordan (2000) stresses that, "… attacks are made on the identity, attitude, behavior, position and relationships of the counterpart" (Jordan, 2000: 4), which was exactly the situation before and during the cyber attack on Sony.

Another characteristic of stage 4 of Glasl's conflict escalation model is that the conflicting parties attempt to affect the image of the opponent internationally. The Sony Hack challenged Sony's image as a big company that can take care of its own and its employees' information and their security and at the same time challenged the image of the United States as a nation state that can protect its business sector. During the cyber attack, sensitive information about employees was leaked - social security numbers, addresses, healthcare information. It is therefore possible to argue that also this characteristic is present in the cyberattack on Sony.

Aim

In stage 4 of Glasl's conflict escalation model, the conflicting parties are becoming stubborn and fixed in their stances to such an extent that they seek to win rather than to find a solution to the conflict through compromises that are acceptable to both sides (Jordan, 2000: 4). The aim of each party's behavior is thus to gain an advantage in the power struggle rather than to find a mutually beneficial solution.

It is thought-provoking that neither North Korea nor Sony sought a mutually acceptable compromise. On North Korea's side, it is possible to argue that the language that what used to describe *The Interview* in the appeal to UN General-Secretary Ban Ki-Moon ("undisguised sponsoring of terrorism, as well as an act of war") reflects an uncompromising perception of the movie, the makers, and anyone supporting them as a threat. The term "terrorism" is difficult to pin-point because most actions are relative, and it is therefore a comprehensive discussion itself. Thus the United Nations has not agreed on a single definition of the term (United Nations Counter-Terrorism Executive Directorate, January 2005). However, referring to the movie as an act of war indicates the seriousness of the situation as well as a perception of it as a threat that must be stopped. One does not negotiate as a reaction to an act of war. Another factor that supports this interpretation is that neither North Korea, nor the hacker group that attacked Sony – "Guardians of Peace" – offered any concessions. On Sony's side no concessions were made either – neither in the plot of the movie, nor its release. Sony did stop the release initially, but according to then SPE CEO Michael Lynton this was only because movie houses refused to run it for fear of the consequences (Weise et al., 2014) – in other words, according to Lynton the movie was only stopped, when there was no longer a market for it, and ultimately it was released despite the threats made by the GOP and the cyber attack. This uncompromising attitude on both sides is in accordance with Glasl's stage 4 of conflict escalation.

Impact

The impact of the cyber attack on Sony in terms of the specific demands of the GOP (the release of *The Interview*) was limited, since the attack only succeeded in delaying the theatrical release. As mentioned, the movie was ultimately released, and on the original release date, too.

The impact in terms of Sony's economic and reputational losses was massive. The attack cost the company $41 million (Springer, 2017: 273) and according to The White House's Council of Economic Advisors, "in addition to expenses for investigation of the attack, IT repairs, and lost movie profits, Sony faces litigation blaming it for poor cybersecurity that exposed employees' private information..." (The White House, The Council of Economic Advisers, February 2018: 16).

However, in examining the impact of the cyber attack on Sony, what is most relevant is the consequences in terms of how it affected the relationship with the victim states – the United States. The United States' response to the attack reveals whether the cyber attack resulted in escalatory measures. An escalation would in turn suggest that the restraint mechanisms that Cyber Restraint Theory speaks of may not be enough to prevent a cyber conflict from escalating, if a state is provoked sufficiently.

In Glasl's stage 4 of conflict escalation, the way of communicating with the opponent is through deniable punishment behavior and "… since the other party cannot respond by openly [and constructively] discussing the incident, retaliatory action is very likely to ensue." (Jordan, 2000: 4). It is possible to argue that the United States responded to the cyber attack on Sony in a manner consistent with the description of stage 4 – by officially imposing economic sanctions on North Korea and by declaring that "… our response to North Korea's attack against Sony Pictures Entertainment will be proportional, and will take place at a time and in a manner of our choosing…" (The White House, 2 January 2015). The last part indicating that the sanctions were not the only response to be expected.

The severity of the sanctions lied in their commercial consequences for North Korea, of course, but also in the fact that this was the first time that the United States sanctioned another state as a result of a cyber attack on a company on American soil (Roberts, 2015). Such a move reflects the seriousness of the overall conflict between the United States and North Korea, because usually sanctions are not the first way of attempting to handle a specific conflict. They were described by the White House as "a response to the Government of North Korea's ongoing provocative, destabilizing, and repressive actions and policies, particularly its destructive and coercive cyber attack on Sony Pictures Entertainment." (The White House, 2 January 2015). Such a description reflects an on-going struggle with North Korea.

North Korea's reaction to the sanctions was further outrage; The North Korean foreign ministry stated: "The persistent and unilateral action taken by the White House to slap 'sanctions' against the [North Korea] patently proves that it is still not away from inveterate repugnancy and hostility towards the [North Korea]…" (Siddique, 2015). It is possible to argue that this reaction reflects anger over measures which are perceived as aggressive and humiliating, thus escalating the conflict from stage 4 to 5. As mentioned in the operationalization section, stage 4 escalates to stage 5, when "… the basic honor of someone is offended repeatedly and deliberately, in particular in a public setting…" (Jordan, 2000: 4).

8.1.3. Interim conclusion: Was the cyber attack of limited severity and impact?

The rhetoric, behavioral patterns, the aim, and the impact of the cyber attack on Sony, reflect that the attack is a stage 4 conflict in terms of Glasl's escalation model. It is thus at the very beginning of the second level of conflict ('Win-Lose'), and it is therefore possible to conclude that the Sony Hack was of limited severity. Although there were material and reputational damages, its impact was also limited compared to the whole spectrum of conflict escalation stages. Even though the conflict between North Korea and the United States escalated quickly from stage 4 to stage 5 after the attack on Sony, it has not escalated further. It is thus possible to conclude that the analysis of the cyber attack on Sony Pictures Entertainment based on Glasl's escalation model has shown that the attack was indeed limited in severity and impact and therefore seems to support the idea that state behavior in cyberspace is restricted.

8.1.4. Discussion: Is the cyber attack on Sony Pictures Entertainment representative of North Korea's general conduct in cyberspace and does this behavior overall reflect restraint?

The cyber attack on SPE was chosen as an example of North Korea's conduct in cyberspace in order to examine whether North Korea's overall behavior reflects cyber restraint. The analysis determined that the Sony Hack reflected a stage 4 conflict (level 2) on Glasl's escalation spectrum and thus was of limited severity and impact. This means that, if the attack on Sony is representative of North Korean conduct in cyberspace, then other cyber actions should reflect the same limited severity and impact.

In order for North Korea's general behavior in cyberspace to be of same severity and impact as the attack on Sony, it would thus have to be within level 2 of Glasl's conflict escalation spectrum, and definitely below what is referred to as the Lose-Lose level of conflict escalation (level 3), which is the most severe. Level 2 is characterized by stages that range from attempting to affect the opponent's image and engaging in deniable punish behavior (stage 4), to public denigration of the opponent (stage 5), and severe threats of violence (stage 6).

Cyber attacks that have been attributed to North Korea have primarily been cases of cyber crime. Some of the most well-known examples are the WannaCry ransomware attack in 2017 and the Bangladesh Bank cyber heist in 2016. During the WannaCry attack, victims were "… asked to pay between $300 (£228) and $600 in ransom with the promise of unlocking the files taken hostage by the malware, of which there were believed to have been around 230,000 computers worldwide." (Gibbs, 2017). During the Bangladesh Bank heist, malware was utilized to compromise SWIFT software which is used in transfers between banks (Schwartz, 2016). Transfer requests were made that led to a heist of $81 million (ibid.). Both cyber attacks were cases of cyber crime and both have led to massive economic losses. Furthermore, they sparked international outrage and frustration over North Korea's continuing crimes in cyberspace, and eventually led to further economic sanctions on North Korea (Bing and Lynch, 2018).
One may be inclined to conclude that these attacks fit the description of stage 7 of Glasl's conflict escalation model, in which attacks target the sanction-potential of the opponent in order to remove the foundation of their political influence. In that case, the severity and impact of the attack on Sony would not represent North Korea's general behavior in cyberspace.

However, it can be argued that, if the aim of North Korea's cyber crime wave was targeting an adversary's economic sanction-potential to affect their influence, the cyber crime attacks would have focused on more internationally influential countries. It would not have targeted countries like Bangladesh, which has limited international power, and probably would have targeted one or a number of specific countries rather than affecting the entirety of 150 countries in one attack alone (BBC, 19 December 2017). Rather, as a UN panel's report has concluded, North Korea seems to seek "… new ways to flout the U.N. sanctions …" (De Luce and Mitchell, 2019).

Placing attacks like the WannaCry and the Bangladesh Bank heist in their political context provides support for this argument. North Korea is under heavy economic sanctions by the UN and has more than once demanded that the sanctions be lifted (Perez and Shortell, 2019). These demands reflect

that the sanctions are frustrating to the North Korean government and its "… desperation for cash is driving a surge in cyberattacks targeting banks and other businesses in the US and around the world…" (ibid.). Thus, when examining North Korea's conduct in cyberspace closely, the context of these cyber attacks suggests that the attacks are not consistent with stage 7 of Glasl's conflict escalation model.

The attacks rather seem like a way to pressure the international community into lifting the economic sanctions on North Korea. Thus, it can be argued that North Korea's general behavior in cyberspace shows examples of actions that signal an ultimatum "… where the counterpart is forced to an either-or decision." (Jordan, 2000: 6). Either lifting the sanctions or enduring the consequences. This is consistent with stage 6 of Glasl's conflict escalation model, where, furthermore, "the threatening party sees only its own demands, and regards the threat as a necessary deterrence in order to block the counterpart from using violence." (ibid). In this case, economic violence in the form of international sanctions. It is thereby possible to argue that the severity of North Korea's general conduct in cyberspace overall reflects stage 6, which is within level 2 of Glasl's conflict spectrum. Since both stage 4 and stage 6 are within level 2 of the conflict escalation model, it can be argued that they exhibit the same level of severity. In other words, it is possible to argue that the attack on SPE, which was also a ransomware attack, is representative of North Korea's overall behavior in cyberspace, which is of limited severity and impact – especially compared to attacks like Stuxnet in 2010 or NotPetya in 2016.

Regarding the discussion of whether North Korea's behavior overall reflects cyber restraint, it may seem as an underestimation to describe its wave of cyber crime as restrained behavior, particularly in the face of the economic losses it has caused to many countries around the world. However, from an international peace perspective, North Korea's actions in cyberspace rather seem like petty crimes – costly and provoking but limited to theft rather than totally destructive actions like the Stuxnet worm that targeted a nuclear plant in Iran.

8.2. Iran's behavior in cyberspace: The cyber attack on Saudi Aramco

In August 2012, the state-owned oil company Saudi Aramco was hit by a destructive cyber attack, in which a malware virus – later named the "Shamoon" virus – infected 30,000 of the company's computers and disabled them beyond repair (Bronk and Tikk-Ringas, 2013). The virus furthermore "erased data on three-quarters of Aramco's corporate PCs — documents, spreadsheets, e-mails, files — replacing all of it with an image of a burning American flag." (Perlroth, 2012).

The attack has since been referred to as "one of the most destructive acts of computer sabotage on a company to date" (Perlroth, 2012) and "the "biggest hack in history" (Pagliery, 2015). It has been attributed to Iran due to the technical features of the Shamoon virus that share commonalities with the "… Wiper malware that had targeted Iran in April 2012, given both destroyed stored data as a method of sabotage." (Anderson and Sadjadpour, 2018). Iran is suspected of having created Shamoon "using the knowledge it gathered from... [the Stuxnet worm and the Flame virus]" (ibid.). Stuxnet and Flame were used in cyber attacks against Iran in 2010 and May 2012, respectively, which makes it likely that Iran sought retaliation by reengineering the cyber weapons used against it and repurposing them.

The political context at the time of the cyber attack on Saudi Aramco was one of strained and aggressive relations between Saudi Arabia and Iran. The rivalry was beginning to re-intensify in 2011 and since manifested in proxy conflicts where "… uprisings across the Arab world caused political instability throughout the region. Iran and Saudi Arabia exploited these upheavals to expand their influence, notably in Syria, Bahrain and Yemen…" (Marcus, 2017). The message that was allegedly left by the attackers on Pastebin.com on August 15, before the cyber attack on Saudi Aramco (https://pastebin.com/HqAgaQRj), suggests that the attack was a means of punishing Saudi Arabia for its foreign policy in the Middle East, thus supporting the suspicion that Iran might be behind the hacker group that took responsibility for the attack.

In addition, Iran had just warned Saudi Arabia "… against delivering additional oil to world markets to compensate for a drop in Iranian oil exports if they [were] hit by sanctions [U.S. sanctions]..." (Faucon et al., 2012). One day earlier, the Saudi oil minister had announced that he would "… boost the kingdom's production by as much as 2.7 million barrels a day, more than Iran exports, if there was a market demand for more oil." (ibid.).

In sum, the political context of the cyber attack on Saudi Aramco in 2012 suggests that Iran was the most likely attacker.

To assess the severity and impact of the cyber attack – and thereby the validity of Cyber Restraint Theory – the following chapter will provide A) a timeline of the attack followed by B) an analysis of the rhetoric and behavior during the attack as well as the aim and the impact of the cyber attack on Aramco based on Glasl's conflict escalation model; C) an interim conclusion of the severity and impact of the Aramco Hack; and finally, D) a discussion that compares the cyber attack with Iran's general conduct in cyberspace and discusses whether such behavior reflects restraint in cyberspace.

8.2.1. Timeline of the cyber attack on Saudi Aramco

In order to understand the severity and impact of the cyber attack on Saudi Aramco, it is important to provide an overview of the events that unfolded during the attack.

The following is a timeline of the attack on the Saudi oil company in August 2012:

- *Phase 1: The Shamoon virus attack and Cutting Sword of Justice*
  On August 15, 2012 at 11:08am local time, the cyber attack took place. The Shamoon virus, "... a self-replicating computer virus enabled an unknown person or persons to commence overwriting files on the hard disks of about 30,000 Windows-based workstations belonging to Saudi Aramco." (Bronk and Tikk-Ringas, 2013: 17). Hours before the cyber attack, a hacker group calling themselves "Cutting Sword of Justice" (CSJ), and describing themselves as anti-oppression, left a message on Pastebin.com announcing that the attack would take place and describing their political motives:

  "We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action.
  One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people." (https://pastebin.com/HqAgaQRj).

Furthermore, the hackers wrote that the cyber attack would destroy 30,000 of Saudi Aramco's computers (ibid.).

On the same day, Saudi Aramco confirmed on its Facebook page that it had "... experienced a disruption in its Information Technology (IT) network" (https://www.facebook.com/Saramcopage). It denied, however, that the disruption had affected "the company's production operations." (ibid.).

- *Phase 2: Saudi Aramco publicly confirms cyber attack*
  On August 16, 2012, Saudi Aramco made another announcement on their Facebook page stating that "On Wednesday, Aug. 15, 2012, an official at Saudi Aramco confirmed that the company has isolated all its electronic systems from outside access as an early precautionary measure that was taken following a sudden disruption that affected some of the sectors of its electronic network. The disruption was suspected to be the result of a virus that had infected personal workstations without affecting the primary components of the network." (https://www.facebook.com/Saramcopage). Afterwards, the Saudi company went offline until another announcement was made on August 26.

- *Phase 3: Threats of further damage*
  On August 23, 2012, Cutting Sword of Justice left another message on Pastebin.com stating that "we are going to make it, next week, once again, and you will not be able by 1% to stop us. Date: 25 august 2012. Time: 21:00 GMT. That's will happen for two reason: 1- you're brutal and selfish to harm any employee just for the sake of expecting. 2- we do hate, hate a lot, arrogance." (https://pastebin.com/WKSk3pmp).

- *Phase 4: Saudi Aramco announces that the company's network is restored*
  On August 26, 2012, Saudi Aramco announced on their Facebook page that normal business had been resumed on August 25, and that "Saudi Aramco has restored all its main internal network services that were impacted on August 15, 2012 by a malicious virus that originated from external sources and affected about 30,000 workstations." (https://www.facebook.com/Saramcopage).

- *Phase 5: Cutting Sword of Justice claim that they still have access to Aramco's network*

On August 29, 2012, Cutting Sword of Justice left a third message on Pastebin.com claiming that they still had access to Saudi Aramco's network. The message read: *"We think it's funny and weird that there are no news coming out from Saudi Aramco regarding Saturday's night. well, we expect that but just to make it more clear and prove that we're done with we promised, just read the following facts -valuable ones- about the company's systems..."* (https://pastebin.com/AtN7dLeW).
The hackers sought to prove it by mentioning information about internet service routers, Aramco CEO Khalid A. Al Faih's email address and password as well as a list of security programs that the company used along with their passwords (ibid.).

8.2.2. Analysis: Severity and impact of the cyber attack

To determine the severity and impact of the cyber attack on Saudi Aramco, the course of events before, during and after the attack will be examined and compared to Glasl's conflict escalation model. Specifically, the rhetoric and behavior surrounding the conflict will be examined, the aim of the cyber attack as well as its impact. By determining which stage of conflict the attack belongs to, it will be possible to determine whether it was of limited severity and impact as Cyber Restraint Theory claims.

Just like with the cyber attack on Sony Pictures Entertainment, to determine the severity of the cyber attack on Saudi Aramco, an examination of the rhetoric surrounding the cyber attack, as well as the behavior of the conflicting parties is vital.

It is possible to argue that level 2 of Glasl's conflict escalation model (stages 4-6) is too mild to characterize the attack on the Saudi oil company. Stage 4 is concerned with attempts of affecting the opponent's image rather than comprehensive and destructive attacks and is thus not consistent with the destructive attack on Saudi Aramco. Likewise, stage 5 does not fit the case at hand, since it is primarily characterized by publicly denigrating the opponent rather than material destruction. Finally, stage 6 is also too different from the cyber attack on the Saudi company. Had the threat of destructive actions by the attackers only been verbal, the attack on Saudi Aramco would have been more consistent with stage 6; The fact that Saudi Arabia's source of international influence – its oil production – was hit, indicates that the conflict between the attackers and Saudi Arabia had already escalated beyond verbal threats – and far beyond friendly negotiation. Therefore, none of stages 4-6 fit the situation of the cyber attack on Saudi Aramco.

Rather, level 3 of Glasl's conflict escalation model is descriptive of the cyber attack on Saudi Aramco. Level 3 is characterized by the fact that the conflicting parties no longer regard the issue as something that can be solved and perceive each other as a threat that undoubtedly threatens their own survival. At this level, the conflict no longer revolves around a concrete and delimited issue, but about the parties' survival. Level 3 attack targets are respectively the opponent's sanction potential (stage 7), political systems that support the opponent's political cohesion (stage 8) and the opponent's existence (9). Stage 9 may, however, be excluded since it describes a situation of total war, where none of the parties are concerned about their own survival as long as they take the opponent down with them (Jordan, 2000: 8). This is clearly not the case, when looking at the cyber attack on Saudi Aramco, because the attackers explain in their message on Pastebin.com on August 15th that the attack is "… a warning to the tyrants of this country and other countries…" (https://pastebin.com/HqAgaQRj). Since a warning is only given in cases, where the attacker wishes to change someone's mind or behavior, the attack on the oil company cannot be described as "total annihilation of the enemy", which is a feature of stage 9.

Since the target of the cyber attack was an oil company, the attack also does not seem to be consistent with the characteristics of stage 8, in which the primary target is the political systems that keep the opponent state coherent and the ultimate goal is to ensure one's own survival (Jordan, 2000: 7).

Rhetoric and behavior

A number of factors indicate that the attack on Saudi Aramco fits stage 7. First, it targeted the world's largest oil company that supplies more than 10% of global oil demand (Olson, 2012) and an oil company in a country, where the "… oil and gas sector accounts for about 50 percent of gross domestic product, and about 70 percent of export earnings (Source: OPEC)." (Export.gov, 11 May 2018). Affecting the oil export of Saudi Arabia would therefore have an effect on both the country's clients, who depend on the oil supply, and the international influence that the Saudi regime holds by virtue of being one of the world's largest suppliers of oil. In other words, the cyber attack targeted the sanction potential of Saudi Arabia. This is in accordance with stage 7 of Glasl's conflict escalation model, where the main strategy of dealing with the adversary is targeting their sanction-potential "… such as destroying or undermining the counterpart's financial resources, juridical status or control functions." (Jordan, 2000: 7).

In the message from CSJ on Pastebin.com on August 15th, the hacking group describes the Saudi regime as "one of the main supporters of… disasters [around the world]… " and a "… corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people." (ibid.). This perception of the Saudi Arabian government is also in accordance with how the conflicting parties perceive and speak of each other in stage 7 of Glasl's conflict escalation model; In this stage, the conflicting parties "… expect the counterpart to be capable of very destructive acts." (Jordan, 2000: 7).

Furthermore, in stage 7, the mistrust, anger, and fear that surround the conflict prevent any constructive communication (ibid.). The messages, left by the CSJ on Pastebin.com, are a means of communication, but it is not constructive, because it is one-way communication attempting to coerce the Saudi regime into changing its conduct rather than a negotiation in which both parties have an equal say in the matter. It is thus possible to argue that the attack reflects that the attackers "… see that it is no longer possible to win [through constructive communication]. It is a lose-lose struggle…" (Jordan, 2000: 7) and therefore seek to deliver a blow to Saudi Arabia's financial resources rather than attempt a friendly negotiation.

To put the cyber attack into its political context, it can be argued that the attack itself is the result of an escalation process in the conflict between Iran and Saudi Arabia. The two rivals have fought one proxy war after another over the years in the region, and the cyber attack on Saudi Aramco can be regarded as another step in their regional power struggle. The attack on Saudi Aramco has been described as "… the first significant use of malware in a hacktivist attack. In the past…most hacktivist attacks were primarily application or DDoS attacks." (Rachwald, 2012). This indicates a dangerously destructive escalation in the field of hacktivism that has not been seen before, which is consistent with stage 7 in Glasl's conflict escalation model, in which "… ethical norms are subsumed under more pressing concerns. At earlier stages the parties exploited gaps in the norms, now they are cast aside if they are bothersome." (Jordan, 2000:6). Likewise, what may be labelled 'emerging norms of how hacktivism is conducted' were cast aside in the attack on Saudi Aramco, and for the first time, malware was used.

Overall, rhetoric and behavior before, during and after the cyber attack on Saudi Aramco is consistent with stage 7 of Glasl's conflict escalation model.

Aim

CSJ's message on Pastebin.com on August 15th states that the Al-Saud regime is "a corrupt regime" and that "an action was performed against Aramco company, as the largest financial source for Al-Saud regime." (https://pastebin.com/HqAgaQRj). Thus, the immediate aim of the cyber attack on Saudi Aramco was to shake the financial foundation of the Saudi Arabian regime and its source of influence on the international scene, which is consistent with stage 7 of Glasl's conflict escalation model.

Furthermore, it is possible to argue that another longer-term aim was to change the foreign policy of the Saudi regime through threats of destruction. As CSJ state, the attack was "… a *warning* to the tyrants of this country…" (https://pastebin.com/HqAgaQRj) – in other words, it was an example of what might happen, if the Saudi regime continues to support "… crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt ..." (ibid.). The last part reveals that the conflict behind the attack is regional and supports the argument that the attack was meant to threaten Saudi Arabia into changing its foreign policy. Since the CSJ states that "the blood of innocent children and people is… " on the Saudi regime's hands (ibid.), it can be argued that the goal of changing Saudi foreign policy is ultimately the survival of other 'innocent children and people'. This is also consistent with stage 7 of the conflict escalation model, in which one wishes to secure one's own survival by attacking the adversary's sources of power.

In sum, the aim of the cyber attack on Saudi Aramco may be divided into three objectives which are consistent with stage 7 of Glasl's conflict escalation model. First, to show the Saudi regime that the foundation of its international influence can and will be contested. Second, to change Saudi Arabia's foreign policy regarding regional conflicts; and third, To secure the attacker's own survival.

Impact

The impact of the cyber attack in terms of changing or affecting the Saudi regime's foreign policy is difficult to assess since the CSJ did not make specific demands – rather, it criticized Saudi Arabia's overall involvement in the region. However, since the cyber attack in 2012, the Saudi regime has been actively involved in regional conflicts, among which are the Qatif conflict in 2017-2019, the

Syrian Civil War which is still ongoing, the involvement in Yemen in 2015, the execution of "a prominent Shia cleric and opposition figure" (Azimi, 2016), Nimr al-Nimr, in 2016 and several other conflicts. This suggests that the cyber attack did not deter Saudi Arabia from continuing its involvement in the region.

The impact in terms of Saudi Aramco's economic and reputational losses was mixed. According to the oil company, the Shamoon virus "… infected personal workstations without affecting the primary components of the network" (https://www.facebook.com/Saramcopage). The extent of the damage, according to the Saudi company, was the disablement of 30,000 computers that were beyond repair, which is consistent with the number that CSJ mentioned in their message on Pastebin.com on the 15th of August. Saudi Aramco stated in a post on the company's Facebook page that the "… primary enterprise systems of hydrocarbon exploration and production were unaffected as they operate on isolated network systems. Production plants were also fully operational as these control systems are also isolated." (ibid.). Furthermore, the company announced in a Facebook post only 11 days after the cyber attack that normal business had been resumed on August 25 (ibid.). However, the attackers contested this by leaving another message on Pastebin.com on August 29 containing company information as proof that they still had access to Saudi Aramco's network (https://pastebin.com/AtN7dLeW). Regardless of the accuracy of Saudi Aramco's announcement, the Facebook post reflects the company's determined attempt to limit the damage to its reputation by indicating that the impact of the cyber attack was limited.

The impact of the cyber attack in terms of how the victim state responded reveals whether the attack led to escalatory retaliation measures. An escalation would in turn suggest that the restraint mechanisms of Cyber Restraint Theory may not be enough to prevent a cyber conflict from escalating, if a state is provoked sufficiently. Conversely, if the victim state did not engage in retaliatory action, it would support the theory of cyber restraint.

Saudi Arabia's response to the cyber attack seems to have been defensive rather than offensive. If any retaliatory cyber actions were taken following the attack on Saudi Aramco, they have not been in the spotlight of the media. Rather, in the years after the attack, Saudi Arabia has worked on improving its cyber security. In fact, "cybersecurity has become one of the fastest growing sectors in Saudi Arabia, with a market value expected to reach $5 billion by 2022. Recent initiatives taken by the Kingdom include the establishment of the National Cybersecurity Authority, the Saudi Federation for Cybersecurity, Programming and UAVs and the Prince Mohammed bin Salman

Higher School of Cybersecurity, Artificial Intelligence and Advanced Technologies." (Kawa, 2019). Thus, this development is not consistent with stage 7 of conflict escalation since Saudi Arabia does not seem to have retaliated in cyberspace. This either reflects how far behind Saudi Arabia is when it comes to cyber security and therefore does not yet have the means to retaliate in the virtual domain, or it supports the idea that states restrain themselves in cyberspace no matter how provoking or threatening the situation may be.

In sum, the impact of the cyber attack is far along the way also consistent with the characteristics of stage 7 of Glasl's conflict escalation model. However, the Saudi regime does not seem to have retaliated in kind in cyberspace, which significantly differs from how conflicting parties react in stage 7.

8.2.3. Interim conclusion: Was the cyber attack of limited severity and impact?

Since stage 7 is part of the final and most severe level of conflict escalation – level 3 – it is at first glance tempting to conclude that the severity and impact of the cyber attack were far from limited, and thus do not reflect restraint. However, the impact of the attack was rather limited and therefore the conflict did not escalate further, which supports Cyber Restraint Theory's claim of restraint in cyberspace.

Regarding the rhetoric surrounding the cyber attack and the behavior of the adversaries, the analysis showed that Iran targeted the sanction potential of Saudi Arabia by going after its oil production. This is an attempt at a rather destructive blow, and thus does not support the claim of limited severity.

Regarding the aim of the cyber attack on Saudi Aramco, it was concluded in the analysis that three objectives were at the heart of the attack: 1) Showing the Saudi regime that the foundation of its international influence can be contested; 2) Changing Saudi Arabia's foreign policy regarding regional conflicts and 3) Securing Iran's own oil export by deterring Saudi Arabia from supplying oil, when Iran cannot.

The impact of the cyber attack in terms of changing or affecting the Saudi regime's foreign policy seemed minimal since the Saudi regime has been actively involved in regional conflicts after the attack.

The impact in terms of Saudi Aramco's economic and reputational losses was also limited. The extent of the damage, according to the Saudi company, was the disablement of 30,000 computers that were beyond repair. Saudi Aramco stated oil production had not been affected.

The impact in terms of Saudi Arabia's response was likewise very limited. Saudi Arabia chose a defensive path in cyberspace rather than an offensive one and thus the conflict did not escalate further.

In sum, the analysis of the cyber attack on Saudi Aramco suggests that while the aim was severe destruction, the impact of the attack was rather limited. Since a case can be severe and still not lead to a dangerous escalation of the conflict, the findings of the analysis seem to support Cyber Restraint Theory in that behavior in cyberspace is restrained.

8.2.4. Discussion: Is the cyber attack on Saudi Aramco representative of Iran's general conduct in cyberspace and does this behavior overall reflect restraint?

The cyber attack on Saudi Aramco was chosen as an example of Iran's conduct in cyberspace to examine whether Iran's overall behavior reflects cyber restraint. The analysis determined that the attack on the Saudi oil company reflected a stage 7 conflict on Glasl's escalation spectrum and was of greater severity but had a limited impact, and therefore supported the theory of restraint in cyberspace after all. This means that, if the attack on Saudi Aramco is representative of Iranian conduct in cyberspace, then other Iranian cyber actions should at least reflect the same limited impact.

It can be argued that although Iran utilized an array of different cyber weapons, its behavior in cyberspace is overall characterized by the same aim and level of severity and impact as the Saudi Aramco attack. Generally, Iran engages in cyber disruption and cyber espionage (Kandell, 2018). These attacks are closely tied to Iran's primary aim in cyberspace, which is the state's survival or maintaining the authoritarian regime (ibid.). Such an aim reflects a severity of cyber attacks that is consistent with stages 7 and 8 of Glasl's conflict escalation spectrum. As has been established, in these stages, either the adversary's sanction-potential or its political coherence is targeted to ensure the attacker's own survival (Jordan, 2000: 7). Already at this point, the general Iranian behavior in cyberspace seems to reflect the same aim – and thereby the same severity of the situation – as in the attack on Saudi Aramco.

The three types of cyber weapons that Iran employs are 1) theft of sensitive information; 2) cyber espionage and reconnaissance and 3) hacking attacks (Kandell, 2018). In the first type of cyber attacks, "… the [hacking] groups Newscatter, Newsbeef, and Charming Kitten [are] known for creating fake accounts on social media platforms to direct users to visit phony websites… to gain access to user information." (ibid.). In the second type of attacks, the hacking groups 'Oil Rig' and 'Helix Kitten' have attacked IT companies and as well as conducted attacks "… at aviation, energy, financial, and governmental institutions." (ibid.). The third type of cyber weapons being used by Iran is hacking attacks on American and Saudi Arabian oil companies. (ibid.). The targets in these attacks further support the argument that Iran's overall conduct in cyberspace falls within stages 7 and 8 of conflict escalation, which suggests that their severity and impact is fairly represented in the case of the Saudi Aramco attack.

The analysis concluded that the cyber attack on the Saudi oil company was of considerable severity, but of modest impact, because Saudi Arabia managed swift damage control. Thus, although the attack was serious, the limited impact seemed to suggest support for Cyber Restraint Theory. Based on the above, it can be argued that the same is the case, when it comes to Iran's general conduct in cyberspace.

8.3. Saudi Arabia's behavior in cyberspace: The case of Jamal Khashoggi

On October 2, 2018, the Saudi Journalist, Jamal Khashoggi, who had been living in the United States since 2017, was assassinated during his visit to a Saudi consulate in Turkey.

Khashoggi had formerly held the position as editor-in-chief of the Saudi daily "al-Watan", but was dismissed in 2003 by the Saudi authorities, when one of his columnists wrote an article that was critical of an Islamic scholar. Khashoggi "… moved to London, bounced around the Middle East, and regularly wrote for the Dubai-based periodical al-Arabiya… [and] eventually relocated to the U.S. in 2017 [where he wrote for The Washington Post]..." (Khamis, 2018).

Jamal Khashoggi was "… an outspoken critic of [Saudi] Crown Prince Mohammed bin Salman…" (Romo, 2019), but according to his friend Omar Abdulaziz, "[Khashoggi] wrote a lot critically before in newspapers but it was only when we started to organize the opposition [with the Bee movement] that [the regime] got upset." (Trew, 2018). The Bee movement is "an "online army" of Saudi activists fighting misinformation cyberwar… [against the Saudi regime]" (ibid.).

8.3.1. Timeline of the assassination of Jamal Khashoggi and following events

The case of Jamal Khashoggi stands out compared to cyber attacks like the one on Sony Pictures Entertainment and Saudi Aramco, where there was a specific and delimitated incident of a hacking that led to immediate losses for the two companies. In Khashoggi's case, the cyber attack came in the form of Saudi surveillance in cyberspace, and a hacking allegedly led to the Saudi regime finding the Saudi emigrant and assassinating him outside of Saudi Arabia. Thus, this case is about how Saudi Arabia used cyber technology to monitor an individual perceived as a threat to the regime and thus were able to find and allegedly assassinate him. The entire conflict will be referred to as a 'cyber attack' in the analysis even though it takes a different form than the ones on Sony and Saudi Aramco, respectively.

Part of what has happened in cyberspace – the monitoring of Khashoggi and hacking of technology – and which has led to the killing of him, has come to light because of the murder. Cyber surveillance, in other words, escalated in Khashoggi's case to an assassination, and since surveillance by definition is secret, it would be difficult to link certain events with specific dates. Therefore, an overview is given below of things that have been said and events that have unfolded after the assassination of Khashoggi. Thus, in order to examine the severity and impact of the cyber

incident, it is necessary to examine actions and statements that have taken place in response to the murder. The following is therefore a timeline of the events following the assassination of Jamal Khashoggi:

- October 2, 2018 – Khashoggi enters Saudi consulate in Turkey and does not leave:
  Saudi journalist Jamal Khashoggi entered the Saudi consulate in Istanbul in order to procure official marriage documents. When he did not leave the consulate, his Turkish fiancée was alarmed. (Turner, 2019; Pandey, 2019).

- October 3, 2018 – Saudi Arabia claims Khashoggi left the consulate alive:
  Saudi Arabia claimed that Khashoggi left the consulate unharmed, (Turner, 2019) while "Turkish presidential spokesman Ibrahim Kalin said the journalist was still in the consulate." (Pandey, 2019).

- October 6, 2018 – Turkish officials believe Khashoggi was murdered inside the consulate:
  Turkish officials stated that they suspected Khashoggi had been killed inside the Saudi consulate, and that they believed that 15 Saudi officials had arrived in Istanbul on October 2, 2018 in order to execute the Saudi journalist (Pandey, 2019; Tuysuz, 2018). Some of the Saudi officials "… appear[ed] to have high-level connections in the Saudi government." (Tuysuz, 2018).

- October 11, 2018 – Business leaders withdraw from investment conference in Saudi Arabia:
  Several business leaders decided to withdraw from an investment conference in Saudi Arabia due to Khashoggi's case (Pilkington, 2018). Furthermore, "British billionaire Richard Branson halted talks over a $1 billion Saudi investment in his Virgin group's space ventures, citing Khashoggi's case." (Pandey, 2019).

- October 15, 2018 – The Saudi consulate in Istanbul is searched:
  The Saudi consulate in Istanbul was searched by Turkish investigators (Smith and Jovanovski, 2018).

- October 19, 2018 – Saudi Arabia claims Khashoggi died inside the consulate in a fistfight:
  Saudi officials admitted that Khashoggi died inside the consulate, claiming that he had been

killed in a fistfight (Pandey, 2019; McKirdy, 2018). In addition, Saudi Arabia's "… public prosecutor said… that 18 people had been detained…. [and] the country is "investigating the regrettable and painful incident."" (Pandey, 2019).

- October 21, 2018 – Saudi Arabia provides a third account of the events at the Saudi consulate: Saudi Arabia stated that Khashoggi was killed in a rogue operation (Pandey, 2019; BBC, 31 October 2018). Officials called it a ""huge and grave mistake," but insisted that the Saudi Crown Prince had not been aware of the murder. Riyadh said it had no idea where Khashoggi's body was." (Pandey, 2019).

- October 21, 2018 – Germany puts weapons exports to Saudi Arabia on hold: Chancellor Angela Merkel stated that Germany would halt weapons deal with the Saudi government, "given the unexplained circumstances of Khashoggi's death." (Pandey, 2019) and "… encourages allies to do the same." (Noack, 2018).

- October 31, 2018 – Turkey concludes that Khashoggi was strangled to death and his remains dissolved in acid: Turkey stated that "in accordance with plans made in advance… Jamal Khashoggi was choked to death immediately after entering the Consulate General of Saudi Arabia… His body was then dismembered and destroyed…" (BBC, 31 October 2018).

- October 2018 – A surge in pro-regime Twitter activity after Khashoggi's disappearance: According to lecturer in the history of the Gulf Arabian Peninsula at Exeter University, Marc Owen Jones, "… there was a huge surge in pro-regime Twitter activity since the disappearance." (Adams, 2018). Allegedly, fraudulent accounts on Twitter, believed to be trolls or bots backed by the Saudi regime, fought the use of hashtags about Khashoggi. Owen Jones argues that "… the activity of these bots removed the hashtag announcing the kidnapping from the list of top trends in Saudi Arabia in just a few hours." (Adams, 2018).

- November 5, 2018 – Saudi Arabia reacts to the international community's call for a transparent investigation: Saudi Arabia informed the UN that those responsible for Khashoggi's murder would be prosecuted. This announcement was a reaction to several states "[raising] the journalist's death before the UN Human Rights Council and [calling] for a transparent

investigation." (Pandey, 2019; Nebehay, 2018).

- November 10, 2018 – Turkey shares audio recordings:
  Turkish president Erdogan stated that audio recordings of the murder of Khashoggi had been shared with Saudi Arabia, U.S., France and Germany (Pandey, 2019; BBC, 11 December 2018).
- November 2018 – Khashoggi's friend reveals his correspondence with Khashoggi:
  Omar Abdulazis "…revealed his correspondence with Khashoggi in November when researchers at the University of Toronto reported his phone had been hacked by military-grade spyware, invented by an Israeli company called NSO Group." (ABC News, 2 December 2018).

- January 3, 2019 – Murder trial begins in Saudi Arabia:
  The trial over Khashoggi's murder began in Saudi Arabia, "… where state prosecutors [said] they [would] seek the death sentence for five of the eleven suspects." (Pandey, 2019).

- January 28, 2019 – UN investigation team in Turkey:
  UN Special Rapporteur Agnes Callamard arrived in Ankara as part of an independent investigation of Khashoggi's death by the UN. (UN Human Rights Office of the High Commissioner, 25 January 2019).

- February 7, 2019 – Results of UN investigation:
  Callamard concluded that the evidence indicated "… that Mr Khashoggi was the victim of a brutal and premeditated killing, planned and perpetrated by officials of the State of Saudi Arabia." (UN Human Rights Office of the High Commissioner,7 February 2019).

- March 7, 2019 – International condemnation:
  Members of the U.N. Rights Council "rebuked" Saudi Arabia for Khashoggi's case. (Cumming-Bruce, 2019; Tamkin, 2019).

8.3.2. Analysis: Severity and impact of the cyber attack

To determine the severity and impact of the cyber attack that led to Khashoggi's assassination, the course of events before and after the murder will be examined and compared to Glasl's conflict escalation model. Specifically, the rhetoric and behavior surrounding the conflict, the aim of the cyber attack as well as its impact will be examined. By determining which stage of conflict Saudi Arabia's actions in cyberspace belongs to, it will be possible to determine whether they were of limited severity and impact as Cyber Restraint Theory claims.

Just like with the cyber attack on Sony Pictures Entertainment and Saudi Aramco, respectively, to determine the severity of the cyber attack on Jamal Khashoggi, an examination of the rhetoric surrounding the cyber attack, as well as the behavior of the conflicting parties is vital.

In this case also, it is possible to argue that level 2 of Glasl's conflict escalation model (stages 4-6) is too mild to characterize the cyber attack. As mentioned, level 2 is the so-called Win-Lose level, where adversaries are still open to communication, albeit it is becoming difficult at stage 6 to have constructive communication. The case of Jamal Khashoggi is however beyond communication since it escalated into an assassination. Therefore, stages 4-6 are not consistent with this case.

Rather, level 3 of Glasl's conflict escalation model is descriptive of the cyber attack on Khashoggi. As mentioned, level 3 is characterized by the fact that the adversaries perceive each other as a threat that undoubtedly threatens their own survival. This is more consistent with the case at hand. More specifically, Khashoggi's case seems to fit stage 8, seeing as stage 7 is about targeting the sanction-potential of the adversary and in stage 9, none of the parties are concerned about their own survival.

Rhetoric and behavior

A number of factors indicate that the cyber attack on Jamal Khashoggi fits stage 8 of Glasl's conflict escalation model. Now, it is important to distinguish between the actual cyber attack and its consequences. The actions that the Saudi regime took in cyberspace that allowed it to monitor Khashoggi's communication channels is the cyber attack itself, while Khashoggi's death was a consequence thereof. Thus, in this case, the conflict is between the Saudi regime and an individual who is central to an opposition movement, which the Saudi regime has an interest in eliminating before it grows too strong to handle.

As an outspoken critic of the Saudi regime and as a central figure in the political opposition, Khashoggi used the press as well as cyberspace as arenas for his attacks on the regime. As his

friend Omar Abdulaziz mentions, "[Khashoggi] wrote a lot critically before in newspapers but it was only when we started to organize the opposition… that [the regime] got upset." (Trew, 2018). Allegedly, Abdulaziz was targeted by "… a similar plan to disappear him in May when prominent Saudi figures tried to lure him to his embassy in Canada. When he refused to go, he was targeted by spyware in an email which tracked his phone calls, after which he was told to stop his online activism." (ibid.). This account of events is supported by Bill Marczak's – a senior research fellow at the Citizen's Lab - conclusion that the software "… was deployed by the Saudi Government and had been used to target at least two dissidents." (ABC News, 2 December 2018).

The Saudi regime's decision to monitor Khashoggi's and Abdulaziz's actions in cyberspace to pinpoint their whereabouts fits the behavioral pattern of stage 8 of Glasl's conflict escalation model. According to the model, "when a party is attacked in a way that threatens to shatter it, it is forced to make strong efforts to suppress internal conflicts." (Jordan, 2000: 7). It is possible to argue that monitoring the founder of and the person funding the Bee Army – and eventually assassinating the latter – are "strong efforts to suppress internal conflicts".

Taking the political context of the cyber attack as well as the assassination of Khashoggi into account, this analysis seems plausible. At this point in time, several regimes in the region had been toppled as part of the Arab Spring. Even though the monarchy in Saudi Arabia has survived so far, anti-government protests did take place in 2011 and 2012, and "there was enough concern among the ruling class to further crack down and suppress opposing voices." (Khamis, 2018). The rise of a Saudi cyber Army of Bees very likely looked like the beginning of an uprising to the Saudi regime – just like the one that took place in Egypt a few years prior and which was started through social media. Thus, several factors support the conclusion that Saudi Arabia's behavior during the Khashoggi case matches stage 8 of conflict escalation model.

Furthermore, stage 8 is characterized by the fact that self-preservation is the only factor that restrains the adversaries' conduct – thus, no ethical or moral standards restrict behavior at this point, even rational self-interest is pushed to the background (Jordan, 2000: 7). This is reflected in the brutality with which cyber tools were utilized in order to find and assassinate Khashoggi. The cyber attack as well as the assassination paint a picture of a regime that is only concerned about its own survival, a regime that sees Khashoggi as a threat and therefore sets all ethical considerations as well as rational self-interest aside to remove the threat. The Khashoggi case has led to international uproar and has affected several business leaders' interest in making economic deals with Saudi

Arabia (Cumming-Bruce, 2019; Tamkin, 2019; Pandey, 2019). The fact that it is a case of an extrajudicial assassination further complicates matters for Saudi Arabia, and has sparked an angry international debate over the legality and appropriateness of using cyberspace to track dissidents living abroad and assassinating them. The fact that the Saudi regime either did not take the international community's reaction into consideration – or perhaps that it underestimated its severity – suggests that even rational self-interest in the form of maintaining good relations with other countries and business partners came second to ensuring the regime's survival. Thus, the Saudi regime's attack on Khashoggi, in cyberspace and outside, reflects a stage 8 conflict in accordance with Glasl's conflict escalation model.

Aim

Consistent with stage 8, the attack in cyberspace targeted the political coherence of the opponent, which in this case is the coherence of the political opposition movement to the Saudi Arabian regime. The regime sought to destabilize the opposition internally by going after an important element of the political opposition – Khashoggi. Khashoggi was important to the movement by virtue of his funding of the so-called Army of Bees (Adams, 2018). It can thus be argued that by eliminating a central figure in the opposition, the Saudi regime hoped to affect its economic as well as political coherence.

Khashoggi "… recently gave $5,000 (£3,800) to "Geish al-Nahla" or the Bee Army, an opposition movement offering cyber protection to Saudi activists needing a safe platform to speak out in the oppressive Kingdom." (Trew, 2018). The Army of Bees has been described as "an online army of Saudi activists fighting a misinformation cyberwar… [against the Saudi regime]" (Trew, 2018). This is done by educating them in the use of "…encrypted browsers and virtual private networks (VPNs)." (ibid.) According to Khashoggi's friend and the founder of the movement, Omar Abdulaziz, the Bee Army "… also give[s] them phone numbers so they can safely activate an anonymous Twitter account. By doing that [it gives] Saudi activists a safe way to express themselves…" (Trew, 2018). In other words, the Bee Army is a political movement that is critical of and wishes to affect the Saudi regime. This is also consistent with stage 8 of Glasl's conflict escalation model, because in this stage, each party in the conflict targets the opponent's political coherence, "… hoping that the very identity of the other side will crumble so that it falls apart through its own internal contradictions and inherent centrifugal forces." (Jordan, 2000: 7).

Thus, the immediate aim of the cyber attack on Khashoggi seems to have been to get information of his communications with the political opposition in order to achieve the longer-term goal of shaking the opposition movement by eliminating its financial support and making an example out of Khashoggi's death. This is consistent with stage 8 of Glasl's conflict escalation model.

In sum, the aim of the cyber attack on Khashoggi may be divided into three objectives which are consistent with stage 8. First, gathering information about the opposition movement and pinpoint Khashoggi's whereabouts. Second, taking strong measures to suppress domestic unrest in Saudi Arabia by surveilling social media and suppressing opposition in cyberspace; and third, to secure the attacker's own long-term survival.

Impact

The impact of the cyber attack in terms of tangible losses cannot be exaggerated. After all, the surveillance in cyberspace led to an individual's death because he was too critical of the Saudi regime. However, this is a rather complicated case, because cyber tools were used to conduct an extrajudicial killing; In other words, besides it being a human rights crime, it is also a case of a government committing a crime on foreign soil. The extended possibilities of surveillance that cyberspace provides were utilized by a foreign government to assassinate an American citizen for exercising his freedom of speech.

The case of Khashoggi stands out, not because extrajudicial killings are unheard of, but rather because we have "… seen leaders across the world emboldened to take acts like this. In [Trump's] first two years [as president], you've seen extrajudicial killings by the North Koreans, by the Russians in Great Britain and now by the Saudis in Turkey." (Transcript of interview between Lakshmi Singh and U.S. Congressman Eric Swalwell, 17 November 2018). Thus, the tangible impact of the cyber attack was loss of life as well as the implications of such an act on the concept of sovereignty inside and outside of cyberspace.

The impact of the cyber attack in terms of how the United States responded – as the state whose citizen was targeted – reveals whether the attack led to escalatory retaliation measures. An escalation would in turn suggest that the restraint mechanisms of Cyber Restraint Theory may not be enough to prevent a cyber conflict from escalating, if a state is provoked sufficiently. Conversely, if the United States did not engage in retaliatory action, it would support the theory of cyber restraint.

The U.S. sent mixed signals regarding the Khashoggi case. Around a month after Khashoggi was assassinated, Trump announced "… that he stood with Saudi Arabia because spoiling relations could negatively impact oil prices, the U.S.' plan to counter Iran in the Middle East and a promise to buy U.S.-made arms." (Turner, 2019). A few months later, Secretary of State Mike Pompeo stated "… that oil prices would not affect America's response to the Khashoggi killing." (ibid.). The U.S. "… and dozens of other countries raised the journalist's death before the UN Human Rights Council and called for a transparent investigation." (Pandey, 2019; Nebehay, 2018). However, the United States has neither promised retaliation in cyberspace nor advocated international sanctions against Saudi Arabia following the attack on an American citizen, which is in stark contrast to the U.S. response to North Korea's cyber attack on a U.S.-based company – Sony Pictures Entertainment. This lack of escalatory measures on the part of the U.S. would suggest that even with the whole world watching in shock over the Khashoggi case, the U.S. has either shown cyber restraint or has prioritized corporate interests over retaliation.

The impact of the Khashoggi case on the international community seems to be a different matter. As mentioned, several countries brought the case of Khashoggi up before the UN Human Rights Council in November 2018 and called for a transparent Saudi investigation of the murder (Pandey, 2019; Nebehay, 2018). Furthermore, the UN conducted its own investigation of the assassination in Turkey in January 2019 (United Nations Human Rights Office of the High Commissioner, 25 January 2019), after which UN Special Rapporteur Callamard concluded in February that "… Khashoggi was the victim of a brutal and premeditated killing, planned and perpetrated by officials of the State of Saudi Arabia." (United Nations Human Rights Office of the High Commissioner,7 February 2019). However, Saudi Arabia has not faced any international sanctions. The Khashoggi case thus did have an impact on the international community, but it has not led to specific political consequences for the state of Saudi Arabia apart from international rebuke (Cumming-Bruce, 2019; Tamkin, 2019). This also suggests that while there is a widespread moral indignation over Khashoggi's death, no serious escalatory cyber measures have been taken, which supports the possibility that cyber restraint is at play.

The impact of the cyber attack in terms of the Saudi opposition movement's response was much like the international community's condemnation – vocal, but without tangible consequences to the Saudi regime. Khashoggi's supporters took to social media using hashtags about Jamal Khashoggi to express their support and spread the word about the assassination. However, the Saudi regime

allegedly fought back seeing as "… hashtags that referred to Khashoggi's case… disappeared from the list of top trends in Saudi Arabia after just a few hours, implying an army of trolls had worked to deliberately bury it. In its place were banal hashtags..." (Trew, 2018). According to activists, the "… troll accounts that used the[se] hashtag[s] were tweeting [them] at them with violent threats and images of torture intended to terrify people out of tweeting about Mr. Khashoggi." (ibid.).

In sum, even though no tangible consequences have befallen Saudi Arabia, there definitely was a political escalation of Khashoggi's case. In other words, the attack on the Saudi journalist did have a massive impact in terms of tangible losses, of the international community's response as well as the Saudi opposition movement's response. The conflict escalated in cyberspace through Khashoggi hashtags but did not lead to retaliation in the virtual domain – not even by hacktivists. This would suggest that cyber restraint might be an explanation.

8.3.3. Interim conclusion: Was the cyber attack of limited severity and impact?

The cyber attack on Khashoggi which lead to his assassination has been identified as a stage 8 conflict, which is the penultimate stage in Glasl's escalation model. This would suggest that the severity and impact of the cyber attack were far from limited.

Regarding the rhetoric surrounding the cyber attack and the behavior of the adversaries, the analysis showed that the Saudi regime monitored Khashoggi's actions in cyberspace to pinpoint his location and assassinate him. When such strong measures are taken in an attempt to suppress political opposition, it is not possible to speak of a limited severity.

Regarding the aim of the cyber attack, the analysis showed that the attack targeted the political coherence of the Saudi opposition movement by killing Khashoggi and thereby removing its financial support. The regime sought to shatter the opposition by going after Khashoggi, who was an important element of the political movement. Such an aim is far more comprehensive and destructive than attempting to negotiate with or even threatening the opponent. Therefore, the aim of Saudi Arabia's conduct also reflects a severe attack.

Regarding the impact of the cyber attack on Khashoggi, it was concluded in the analysis that there was a massive political escalation. The attack on the Saudi journalist did have a considerable impact in terms of tangible losses, of the international community's response as well as the Saudi opposition movement's response, even if it has not led to specific sanctions against the perpetrators.

However, no retaliatory actions were taken against Saudi Arabia, which suggests that even though Khashoggi's case was a serious human rights violation that sparked international outrage, cyber restraint might be a plausible theory.

In sum, the analysis of the cyber attack on Jamal Khashoggi suggests that while the severity of the attack was not limited, its impact was. Since a case can be that severe and still not lead to a dangerous escalation of the conflict, the findings of the analysis seem to support Cyber Restraint Theory in that behavior in cyberspace is restrained.

8.3.4. Discussion: Is the case of Jamal Khashoggi representative of Saudi Arabia's general conduct in cyberspace and does this behavior overall reflect restraint?

The cyber attack on Jamal Khashoggi was chosen as an example of Saudi Arabia's conduct in cyberspace in order to examine whether Saudi Arabia's overall behavior reflects cyber restraint. The analysis determined that the attack on Khashoggi reflected a stage 8 conflict on Glasl's escalation spectrum and was thus of great severity. It was also concluded that the impact on Khashoggi's life was massive and in terms of political escalation it was likewise considerable. Thus, the attack was not consistent with Cyber Restraint Theory's claim of limited severity and impact. This means that, if the attack on Khashoggi is representative of Saudi Arabian conduct in cyberspace, then other cyber actions should reflect the same great severity and impact.

Saudi Arabia is an example of the fact that "cyber capabilities are not merely utilized by [states] for… international and regional warfare and confrontation…. [but also] for internal repression." (Kandell, 2018). Saudi Arabia's engagement in international cyber attacks has been modest to date, because "despite the 70 percent Internet penetration and expanded mobile use, e-commerce is still underdeveloped." (Hathaway et al., 2017: 4). However, the Saudi youth is "… among the most active social media users in the world – and largest adopters of Twitter in the Arab region… [and] a large number of the population is increasingly turning to circumvention tools, such as Hotspot Shield, to access banned content and services." (Hathaway et al., 2017: 3). In other words, cyberspace has opened up the country to international sources of information and new possibilities of exchanging ideas. It has also allowed the Saudi people platforms, where they can express their political views – some of them critical of the regime.

In fact, political protests took place in Saudi Arabia in 2011 over "… poor infrastructure after deadly floods swept through Saudi Arabia's second biggest city." (Reuters, 29 January 2011). The call for action was sent over messages on smart-phones (ibid.) and "more than 17,000… backed a call on Facebook to hold two demonstrations…" (Laessing, 2011). This illustrates – just like other cases in the Arab Spring – that new possibilities of collective mobilization were provided in cyberspace, and that it was becoming a problem for the Saudi regime. At the time, Saudi Arabia announced a ban on marches (ibid.), which reflects growing worries over a political revolution.

This has been a growing challenge for the Saudi regime, which is one of the few governments in the Arab region that were not toppled during the Arab Spring. Since the downfall of other governments in the region came through social media, the Saudi government learned the lesson and directed its cyber capabilities inwards, surveilling its own people on social media to suppress potential political unrest. The cyber attack on Khashoggi is thus a representative example of Saudi Arabia's conduct in cyberspace, which may be described as a stage 8 situation on Glasl's conflict escalation spectrum.

Regarding whether the Saudi regime's behavior overall reflects cyber restraint, it can be argued that since the Khashoggi case was determined as a severe cyber attack with a massive impact and it represents Saudi Arabia's general conduct in cyberspace, then the kingdom's actions are not consistent with Cyber Restraint Theory.

9. Overall discussion: Does the overall behavior of North Korea, Iran and Saudi Arabia in cyberspace pose a threat to international peace?

Not all three cases' behavior was consistent with Cyber Restraint Theory's claim that cyber attacks will be of limited severity and impact and therefore the question remains: Is North Korean, Iranian and Saudi Arabian conduct in cyberspace a threat to international peace? There are two sides to this debate, and at its core it is a discussion of whether the issues of linking governments with specific cyber attacks allows states too much room for maneuver in the virtual domain, or whether it is the lack of ways to hold such states accountable that is the real threat to international peace.

On one hand, it can be argued that the three states can "punch above their weight" in cyberspace without fear of escalation in the conventional physical domain, because of how difficult it is to prove a link between state-sponsored cyber attacks and the state behind them – the so-called Problem of Attribution (Goutam, 2015; Fischerkeller and Harknett, 2017). According to this trail of thought North Korea, Iran and Saudi Arabia may be tempted by the new power possibilities that such untraceability (or anonymity) offers in cyberspace, and if their behavior is not unconditionally restrained by fear of escalation, they can indeed be considered a (potential) threat to international peace.

In such a case, states would be able to conduct unscrupulous cyber activities without fear of detection, thus making states bolder and arguably inclined to cybercrime and possibly destruction (ibid.). In turn, the lack of accountability makes North Korea, Iran and Saudi Arabia dangerous, because their actions would not be restrained by a consideration of the consequences.

Seeing as North Korea and Iran are pursuing Weapons of Mass Destruction and that they consider the West an enemy, it could thus be argued that a lack of accountability for their actions in cyberspace makes their pursuits a threat to international peace. For Saudi Arabia, the lack of accountability for its actions in the virtual domain would mean that the kingdom's actions towards its own population would be subject to no restrictions or considerations of human rights. While domestic human rights issues may not directly affect international peace, the Saudi regime's boldness in targeting a former Saudi citizen on a NATO ally's soil – a citizen that resided in the United States – may indicate that the Problem of Attribution is allowing states like Saudi Arabia to push the boundaries of the concept of sovereignty. In other words, targeting an individual on foreign soil is a controversial act, because it possibly infringes on another state's sovereignty and it sets a dangerous precedence that may be considered a threat to international peace.

On the other hand, the counterargument is that even though the virtual domain opens up for new ways of state interactions, the so-called nature of cyberspace – including the Problem of Attribution – is not without its limits seeing as political context often provides a basis for linking a cyber attack to possible attackers in the virtual domain (Valeriano and Maness, 2015: 46).

Apart from technically tracing a cyber attack, it is possible to argue that political context also provides a solution to the Problem of Attribution. Like the analyses established, in all three cases – the Sony Hack, the attack on Saudi Aramco and the case of Jamal Khashoggi – there was a foreign policy issue surrounding the attacks in cyberspace. In other words, such cyber attacks do not happen politically unmotivated and in a vacuum (ibid.). Cyber weapons may thus be considered a tool that states use to support their foreign policy pursuits; therefore, analyzing the political context as well as the technical circumstances of the cyber attack, would help diminish the room for political maneuver that the so-called Problem of Attribution provides (ibid.).

However, it is also possible to argue that establishing a link between cyber attacks and specific governments does not in itself ensure that states will be more restrained in cyberspace and thus not a threat to international peace. While attribution would officially justify international sanctions, it can be argued that the lack of internationally recognized laws or norms of state behavior in cyberspace is the real liability. This is because a lack of an internationally accepted understanding of what is appropriate behavior in cyberspace and what is not, leaves too much room for "interpretation" or maneuvering by states pursuing their foreign policy goals in cyberspace. In other words, it allows for more clashes between states and thereby for international conflict. It also means that holding states accountable for their conduct in cyberspace will be based on normative judgement rather than impartiality, if no common ground rules have been laid.

One argument in the debate about cyber conflict is that such ground rules have not yet developed – neither in the form of international laws nor internationally recognized norms in cyberspace (e.g. Wheeler, 2018). North Korean cyber crime, Iranian espionage and disruption as well as Saudi Arabian cyber surveillance can, in this light, be perceived as evidence that norms have not yet developed in cyberspace; that this kind of conduct is taking place because there is no common understanding of what is to be considered acceptable behavior (ibid.). In contrast, the international outrage over the cyber attacks that have been attributed to these states suggests otherwise; if there is international outrage, there must be a common understanding that such behavior is beyond what is acceptable.

The discussion of whether North Korea, Iran and Saudi Arabia pose a threat to international peace is thus highly a matter of perspective. It is, however, possible to argue that it is too early for North Korea, Iran and Saudi Arabia to pose a threat in cyberspace, because just like the academic community is still developing theories of cyber conflict, it can be argued that states are also still learning of the new power possibilities as well as the limits of actions in cyberspace. While these new possibilities are actively being tested by the three states at this point in time – often by challenging the United States – it can be argued that in two of the three cases in this thesis some measure of cyber restraint was established, which suggests that states do not take cyber conflict lightly.

Furthermore, even though the analyses showed that Cyber Restraint Theory's generalizing approach is questionable – that states are not unconditionally restrained in cyberspace – they also revealed that North Korea and Iran have indeed acted in a somewhat restrained manner, which may suggest that states that are under international scrutiny, do not have the same freedom of navigation in the virtual domain as states that are considered allies.

North Korean, Iranian and Saudi Arabian conduct in the virtual domain is thus not a threat to international peace at this point in time, but the analyses showed that especially Saudi Arabia has already reached a high severity of conflict behavior in cyberspace, and based on this, it is possible to argue that such behavior may continue and escalate further, if common norms regarding state behavior in cyberspace are not developed and agreed upon explicitly.

10. Conclusion

This thesis sought to examine whether states that are under economic and political scrutiny and in a desperate situation conduct themselves in a restrained manner in cyberspace. North Korea and Iran where chosen as two states that are considered 'rogue' and are thus heavily sanctioned by the international community. Saudi Arabia was chosen because of its dual position as an ally to Western countries and an authoritarian state that builds on values that are at odds with liberal democratic values.

The research question of this thesis was: Is North Korean, Iranian and Saudi Arabian conduct in cyberspace characterized by restraint or do these states pose a threat to international peace?

For each of the three states, a cyber attack which has been attributed to them was chosen to exemplify their respective behaviors in cyberspace. Thus, the hacking of Sony Pictures Entertainment in 2014 (or just 'Sony Hack') was selected as an example of North Korea's conduct in the virtual domain; the cyber attack on Saudi Aramco in 2012 was chosen to represent Iran's behavior; and the case of Jamal Khashoggi in 2018 was selected as an example of Saudi Arabia's conduct in cyberspace.

Friedrich Glasl's nine-stage conflict escalation model was applied to the three cyber attacks in order to examine whether Cyber Restraint Theory's claim, that cyber attacks will continue to be of limited severity and impact, is valid. The circumstances surrounding each cyber attack were analyzed alongside the actual events during the attacks. Thus, rhetoric/behavior, the aim of the cyber attack as well as its impact were examined to determine the severity and impact.

The analysis of North Korean behavior in cyberspace identified the Sony Hack as a stage 4 conflict. This was based on the attackers' behavioral pattern, the communications between the attackers (both the actual hacker group and North Korean officials) and the extent to which the cyber attack escalated politically and led to retaliation in cyberspace. The findings were consistent with stage 4, which is characterized by mainly six distinctive features: 1) deniable punishment behavior; 2) Both the attacker and the victim consider their own actions as a response to the adversary's actions and intentions; 3) The character of the opponent is perceived as the central issue in the conflict rather than irreconcilable political standpoints; 4) The conflicting parties attempt to affect the image of the opponent internationally; 5) The adversaries seek to win rather than to find a mutually beneficial solution; and finally 6) The victim of an attack retaliates, thereby risking a further escalation of the

situation. Since the Sony Hack was considered a stage 4 conflict, its severity as well as its impact was determined as limited. The conclusion of the analysis was thus that the cyber attack supported the premises of Cyber Restraint Theory.

The analysis of Iran's conduct in cyberspace identified the cyber attack on the state-owned Saudi oil company Saudi Aramco as a stage 7 conflict, because it targeted the sanction-potential of Saudi Arabia. Stage 7 is primarily characterized by three features: 1) The adversaries target each other's sanction-potential, and 2) Ethical norms become a secondary concern to the opposing parties; and 3) There is no longer any constructive communication between the opposing parties.

It was concluded that the cyber attack targeted a state-owned oil company in a country where the basis of international influence is the oil production. In other words, it targeted the sanction-potential of Saudi Arabia. At this stage there was no constructive communication between the attackers and the oil company; although the hacker group that claimed responsibility of the attack communicated with Saudi Aramco, their messages were an announcement of the attack, rather than an attempt to negotiate. While the severity of this cyber attack was determined to be high, the impact was very limited because Saudi Aramco quickly contained the damages and no retaliatory actions seem to have been taken by Saudi Arabia. The conclusion of this analysis was that the attack, while challenging the premises of Cyber Restraint Theory because of its severity, did not definitively disprove it because after all, Saudi Arabia did not retaliate.

The analysis of Saudi Arabia's conduct in cyberspace identified the cyber attack, leading to the assassination of the Saudi activist Jamal Khashoggi, as a stage 8 conflict. In stage 8 the characteristic behavior of the adversaries is 1) targeting each other's political coherency by targeting political structures, and 2) the adversaries take strong measures to suppress domestic unrest. It was argued that by being part of the online opposition to the Saudi regime, Khashoggi was actively attempting to shake the Saudi government. Likewise, the cyber surveillance that led to the assassination of Khashoggi was considered an attack on the political cohesion of the online opposition movement, the "Bee Army". The severity as well as the impact of the cyber attack were considered very high, because it led to a loss of life as well as a challenge to a NATO ally's authority, since the assassination took place in Turkey. The conclusion was therefore that the case of Jamal Khashoggi challenged the premises of Cyber Restraint Theory, thereby indicating that states are not unconditionally restrained in their conduct in cyberspace.

Since cyber war was defined, in this thesis, by the loss of life, it is also possible to conclude, based in the analyses, that the Sony Hack and the cyber attack on Saudi Aramco are not examples of cyber war, but rather of cyber conflict between regional rivals. The case of Jamal Khashoggi, however, led to an assassination and can thus be characterized as a cyber war between the Saudi regime and the political opposition movement – the Bee Army.

The three analyses were raised to a higher analysis plane by relating each cyber attack to respectively North Korea's, Iran's and Saudi Arabia's general conduct in cyberspace. Thus, it was argued that each of these attacks do indeed represent the severity and impact of each state's general behavior in the virtual domain. This places North Korea's conduct of cyber crime on a restrained or limited stage 4, Iran's behavior of espionage and disruption on a more challenging stage 7, and Saudi Arabia's conduct of domestic cyber surveillance to suppress political opposition on an alarming stage 8.

These conclusions to the three analyses were related to the question of whether North Korea, Iran and Saudi Arabia's behavior in cyberspace is restrained; the discussion took the findings a step further by offering two perspectives in the debate of whether the three states' behavior is an international problem – whether it is a threat to international peace. One perspective was that, since Cyber Restraint Theory is not unconditionally valid in the cases of Iran and Saudi Arabia, then at least these two states were likely to take advantage of the new power possibilities in cyberspace which are based on the Attribution Problem. In other words, the issue of attributing cyber attacks to specific governments will be taken advantage of in the two states' pursuit of their goals in cyberspace. The other perspective considered the 'Problem of Attribution' as a diminishing issue due to technological developments as well as the benefits of contextual analysis. Therefore, especially Iran and Saudi Arabia were not considered a threat to international peace due to the Problem of Attribution – rather, it was the lack of international cooperation in the form of common norms regarding state behavior in the virtual domain that gives the two states room for dangerous maneuver, and thus can be considered a threat to international peace.

While the analyses showed that especially Iranian and Saudi Arabian behavior, respectively, is not restrained in cyberspace, the discussion illustrated that whether the two states are a threat to international peace is a matter of perspective. This answers the research question: Is North Korean, Iranian and Saudi Arabian conduct in cyberspace characterized by restraint or do these states pose a threat to international peace?

11. Bibliography

ABC News (2 December 2018). Jamal Khashoggi's private messages describe growing fear of 'beast Pac-Man' Saudi Prince. *ABC News*: https://www.abc.net.au/news/2018-12-03/khashoggi--called-saudi-prince-salman-beast-pac-man-in-whatsapp/10576252

Adams, D. (2018). Was Jamal Khashoggi a Victim of a Saudi Cyberwar? *Digit*: https://digit.fyi/jamal-khashoggi-casualty-in-saudi-cyberwar/

Albert, E. (2019). What to Know About Sanctions on North Korea. *Council on Foreign Relations*: https://www.cfr.org/backgrounder/what-know-about-sanctions-north-korea

Alford, L. D. (2000). Cyber warfare: protecting military system. *Aquisition Review Quarterly* (Spring 2000), pp. 100-120.

Anderson, C. and Sadjadpour, K. (2018). *Iran's Cyber Threat: Espionage, Sabotage, and Revenge.* Carnegie Endowment for International Peace: https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

Arquilla, J. (2012). Cyberwar Is Already Upon Us. *Foreign Policy*: https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/

Azimi, S. (2016). Iran-Saudi tensions erupt in 'cyberwar'. *BBC*: https://www.bbc.com/news/world-middle-east-36438333

BBC News (19 October 2018). Jamal Khashoggi: Saudi murder suspect had spy training. *BBC News*: https://www.bbc.com/news/world-middle-east-45918610

BBC News (31 October 2018). Khashoggi murder: Turkey gives official details of Saudi writer's death. *BBC News:* https://www.bbc.com/news/world-europe-46049204

BBC News (11 December 2018). Jamal Khashoggi: All you need to know about Saudi journalist's death. *BBC News*: https://www.bbc.com/news/world-europe-45812399

BBC News (19 December 2017). Cyber-attack: US and UK blame North Korea for WannaCry. *BBC News*: https://www.bbc.com/news/world-us-canada-42407488

BBC News (3 January 2019). Jamal Khashoggi murder trial opens in Saudi Arabia. *BBC News*: https://www.bbc.com/news/world-middle-east-46747332

Benner, K.; Mazzetti, M.; Hubbard, B. and Isaac, M. (2018). A toll army and a Twitter insider. *The New York Time*: https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html

Bing, C. and Lynch, S. N. (2018). U.S. charges North Korea hacker in Sony, WannaCry cyberattacks. *Reuters*: https://www.reuters.com/article/us-cyber-northkorea-sony/u-s-charges-north-korean-hacker-in-sony-wannacry-cyberattacks-idUSKCN1LM20W

Breene, K. (2016). Who are the cyberwar superpowers? World Economic Forum: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

Brickley, J. (2012). Defining Cyberterrorism: Capturing a broad range of activities in cyberspace. *CTC Sentinel* (August 2012), Vol. 5, No. 8: https://ctc.usma.edu/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace/

Bronk, C and Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. *Survival* 55(2).

Bunkall, A. (2019). Iran conducted 'major cyber assault' on key UK infrastructure. *Sky News*: https://news.sky.com/story/iran-conducted-major-cyber-assault-on-key-uk-infrastructure-11676686

Cambridge Dictionary: https://dictionary.cambridge.org/dictionary/english/troll-factory

CBS News (12 May 2017). Global cyberattack strikes dozens of countries, cripples U.K. hospitals. *CBS News*: https://www.cbsnews.com/news/hospitals-across-britain-hit-by-ransomware-cyberattack/

Coats, D. R. (2019). *Statement for the record - Worldwide threat assessment of the US intelligence community*, Senate Select Committee on Intelligence.

Cumming-Bruce, N. (2019). Saudi Arabia Rebuked for First Time by Fellow Members of U.N. Rights Council. *The New York Times*: https://www.nytimes.com/2019/03/07/world/middleeast/saudi-arabia-human-rights-abuses.html

De Luce, D. and Mitchell, A. (2019). U.N. report: North Korea evading sanctions by buying oil, selling coal, hacking banks. *CNBC*: https://www.cnbc.com/2019/03/12/un-report-north-korea-evading-sanctions-by-buying-oil-hacking-banks.html

Dewey, T.; Kaden, J.; Marks, M.; Matsushima, S. and Zhu, B. (2012*). The Impact of Social Media on Social Unrest in the Arab Spring*, Stanford University.

Doffman, Z. (2019). Cyber Attacks: 50% Of Those Hit Are Hit Monthly, And Iran Hits Hardest Of All. *Forbes*: https://www.forbes.com/sites/zakdoffman/2019/04/03/u-k-cyber-attacks-50-of-those-hit-are-hit-monthly-and-iran-hits-hardest-of-all/#38a706eb55ab

Easton, G. (2010). Critical realism in case study research. *Industrial Marketing Management* 39, pp. 118–128: http://www.mega-project.eu/assets/exp/resources/critical_realism_-_easton_1.pdf

Edirisingha, P. (2012). Interpretivism and Positivism (Ontological and Epistemological Perspectives): https://prabash78.wordpress.com/2012/03/14/interpretivism-and-postivism-ontological-and-epistemological-perspectives/

Export.gov (11 May 2018). Saudi Arabia – Oil and Gas: https://www.export.gov/article?id=Saudi-Arabia-oil-and-gas

Faucon, B.; Sharma, R. and Lee, Y. (2012). Iran Confronts Saudis on Oil Offer. *The Wall Street Journal*: https://www.wsj.com/articles/SB10001424052970204468004577166870499947012

FBI National Press Release (19 December, 2014). Update on Sony Investigation. FBI: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

Fischerkeller, M. P. and Harknett, R. J. (2017). Deterrence is Not a Credible Strategy for Cyberspace. *Orbis*. 61. 10.1016/j.orbis.2017.05.003.

Fixler, A. (2019). Are we underestimating Iran's cyber capabilities? *The Hill:* https://thehill.com/opinion/cybersecurity/433431-are-we-underestimating-irans-cyber-capabilities

Freedom on the Net 2018, Saudi Arabia: https://freedomhouse.org/report/freedom-net/2018/saudi-arabia

Fixler, A. and Cilluffo, F. (2018). *Evolving Menace - Iran's use of cyber-enabled economic warfare*. FDD Press, a division of the Foundation for Defence of Democracies: https://www.fdd.org/wp-content/uploads/2018/11/REPORT_IranCEEW.pdf

Danish Defence Intelligence Service (2019). Threat Assessment - The Cyber Threat Against Denmark 2019. Centre for Cyber Security: https://fe-ddis.dk/cfcs/publikationer/Documents/The-Cyber-Threat-Against-Denmark-2019.pdf

Garamone, J. (2018). Cyber Tops List of Threats to U.S., Director of National Intelligence Says. U.S. Department of Defense: https://dod.defense.gov/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/

Gartzke, E. (2013). The Myth of Cyber War. *International Security*, Vol. 38 (2): 41-73.

George, A. and Bennett, A. (2005). *Case studies and theory development in the social sciences*. Cambridge, MIT Press.

Goertz, G., and Mahoney, J. L. (2012). Concepts and measurement: Ontology and epistemology. *Social Science Information*, 51(2), 205-216.

Gomez, M. A. N. (2018). In cyberwarm there are some (unspoken) rules. *Foreign Policy*: https://foreignpolicy.com/2018/11/06/in-cyberwar-there-are-some-unspoken-rules-international-law-norms-north-korea-russia-iran-stuxnet/

Goutam, R. K. (2015). The Problem of Attribution in Cyber Security. *International Journal of Computer Applications* (0975 – 8887) Vol. 131, No.7: citeseerx.is t.psu.edu/viewdoc/download?doi=10.1.1.735.4528&rep=rep1&type=pdf

Gibbs, S. (2017). WannaCry: hackers withdraw £108,000 of bitcoin ransom. *The Guardian:* https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom

Hathaway, M.; Spidalieri, F. and Alsowailm, F. (2017). *Kingdom of Saudi Arabia - Cyber readiness at a glance.* Potomac Institute for Policy Studies.

Hersh, S. M. (2010). The online threat - Should we be worried about cyber war? *The New Yorker*: https://www.newyorker.com/magazine/2010/11/01/the-online-threat

Hirst, J. (2012). The free expression problems of authoritarian regimes. George W. Bush Presidential Center: https://www.bushcenter.org/publications/articles/2012/09/the-free-expression-problems-of-authoritarian-regimes.html

Holm, L. (2017). *Cyber attacks and coercion in the digital era – A qualitative case analysis of the North Korean cyber attack on Sony Pictures*. Department of Government, Uppsala University.

Human Rights Watch, World Report 2019: Saudi Arabia - Events of 2018: https://www.hrw.org/world-report/2019/country-chapters/saudi-arabia

Jackson, P. T. (2011): *The Conduct of Inquiry in International Relations. Philosophy of Science and Its Implications for the Study of World Politics*. Abingdon, Routledge, pp. 24-40.

Jordan, T. (2000): Glasl's Nine-Stage Model Of Conflict Escalation. University of Gothenburg: https://www.researchgate.net/publication/265452970_Glasl's_Nine-Stage_Model_Of_Conflict_Escalation

Kandell, S. (2018). Iranian Cyber Warfare: State Repression and International Retaliation. *Compass*: https://wp.nyu.edu/compass/2018/11/13/iranian-cyber-warfare-state-repression-and-international-retaliation/

Kawa (2019). Saudi Arabia faces hackers. *Kawa*: https://kawa-news.com/en/saudi-arabia-faces-hackers/

Khamis, S. (2018). Jamal Khashoggi's murder finally brings media attention to plight of Arab world's exiled critics. *The Conversation*: https://theconversation.com/jamal-khashoggis-murder-finally-brings-media-attention-to-plight-of-arab-worlds-exiled-critics-105705

King, G.; Keohane, R.O.; Verba, S. (1994). *Designing Social Inquiry*. Princeton University Press.

Klare, M. (1995). *Rogue States and Nuclear Outlaws: America's Search for a New Foreign Policy*. Hill and Wang.

Klotz, A. and Prakasch, D. (2006). *QualitativeMethods in International Relations. A Pluralist Guide*. Palgrave.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem, in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: National Defense UP, 2009).

Laessing, U. (2011). Saudi Arabia says won't tolerate protests. *Reuters*: https://www.reuters.com/article/us-saudi-protests/saudi-arabia-says-wont-tolerate-protests-idUSTRE72419N20110305

Langner, R. (28 October 2016). Cyber Power - An emerging factor in national and international security. *Horizons*: https://www.cirsd.org/en/horizons/horizons-autumn-2016--issue-no-8/cyber-power-an-emerging-factor-in-national-and-international-security

Langner, R. (November 2013): To Kill a Centrifuge - A technical analysis of what Stuxnet's creators tried to achieve. The Langner Group: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Lawrence, A. (2007). Imperial Peace of Imperial Method? Skeptical Inquiries into Ambiguous Evidence for the 'Democratic Peace, in Richard Ned Lebow and Mark Irving Lichbach (eds.), *Theory and Evidence in Comparative Politics and International Relations*, Basingstoke, Palgrave, pp. 199-228.

Lewis, J. A. (2010). The Cyber War Has Not Begun. *Center for Strategic and International Studies:* http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf

Lynn, W. J. III (2010). Defending a New Domain - The Pentagon's Cyberstrategy. *Foreign Affairs*: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Marcus, J. (2017). Why Saudi Arabia and Iran are bitter rivals. BBC: https://www.bbc.com/news/world-middle-east-42008809

McGuffin, C. and Mitchell, P. (2014). On domains: Cyber and the practice of warfare. *International Journal*, Vol. 69, No. 3, pp. 394-412.

McKirdy, E. (2018). Jamal Khashoggi died in fistfight at Istanbul consulate, Saudi Arabia claims. *CNN*: https://edition.cnn.com/2018/10/19/world/saudi-arabia-khashoggi-intl/index.html

Message left on Pastebin.com by the attackers (15 August 2012): https://pastebin.com/HqAgaQRj

Message left on Pastebin.com by the attackers (27 August 2012): https://pastebin.com/AtN7dLeW

Nebehay, S. (2018). Saudi Arabia tells U.N. it will prosecute Khashoggi killers. Reuters: https://www.reuters.com/article/us-saudi-rights-un/saudi-arabia-tells-u-n-it-will-prosecute-khashoggi-killers-idUSKCN1NA17N

Noack, R. (2018). Germany halts arms deal with Saudi Arabia, encourages allies to do the same. *The Washington Post*: https://www.washingtonpost.com/world/2018/10/22/germany-its-allies-well-halt-future-arms-sales-saudi-arabia-until-we-have-clarity-khashoggi-so-should-you/?utm_term=.911fa0c5d12e

Nye, J. S. Jr. (2010). Cyber Power, Belfer Center for Science and International Affairs: https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf

Nye, J. S. Jr. (2011). Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly (Winter): 18-38.*

Nye, J. S. Jr. (2017). Deterrence and Dissuasion in Cyberspace. *International Security,* Vol. 41, No. 3 (Winter 2016/17), pp. 44–71.

Olson, P. (2012). The Day a Computer Virus Came Close To Plugging Gulf Oil. *Forbes*: https://www.forbes.com/sites/parmyolson/2012/11/09/the-day-a-computer-virus-came-close-to-plugging-gulf-oil/#471b877934d8

O'Reilly, K. P. (2007). Perceiving Rogue States: The Use of the "Rogue State" Concept by U.S. Foreign Policy Elites. *Foreign Policy Analysis*, Vol. 3, No. 4, October 2007, pp. 295–315.

Ottis, R and Lorents, P. (2011). Cyberspace: Definition and implications. 5th European Conference on Information Management and Evaluation, ECIME 2011, pp. 267-270.

Pagliery, J. (2015). The inside story of the biggest hack in history. *CNN*: https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html

Pandey, A. (2019). UN expert: Jamal Khashoggi killing planned by Saudis. *DW*: https://www.dw.com/en/un-expert-jamal-khashoggi-killing-planned-by-saudis/a-47414594

Pellerin, C. (2010). Cyberspace is the new domain of warfare. U.S. Air Force: https://www.af.mil/News/Article-Display/Article/115277/cyberspace-is-the-new-domain-of-warfare/

Perlroth, N. (2012). In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. *The New York Times*: https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

Perez, E. and Shortell, D. (2019). North Korean-backed bank hacking on the rise, US officials say. *CNN*: https://edition.cnn.com/2019/03/01/politics/north-korea-cyberattacks-cash-bank-heists/index.html

Peterson, A. (2014). The Sony Pictures hack, explained. The Washington Post: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.5c317455cddc

Pilkington, E. (2018). Sir Richard Branson suspends Saudi business talks over Khashoggi affair. *The Guardian*: https://www.theguardian.com/business/2018/oct/11/sir-richard-branson-suspends-saudi-business-talks-over-khashoggi-affair

Pomerantz, D. (2014). Sony Will Release 'The Interview' Online. *Forbes*: https://www.forbes.com/sites/dorothypomerantz/2014/12/24/sony-will-release-the-interview-online/

Pope, L. (2008). *Cyber-Terrorism and China*, United States Marine Corps. Command and Staff College, Marine Corps University.

Rachwald, R. (2012). The Significance of the Aramco Hack. *Imperva* https://www.imperva.com/blog/the-significance-of-the-aramco-hack/

Reardon, R. and Choucri, N. (2012). *The Role of Cyberspace in International Relations: A View of the Literature*. Prepared for the 2012 ISA Annual Convention.

Reuters (29 January 2011). Dozens detained in Saudi over flood protests. *The Peninsula*: https://www.webcitation.org/5w9qUZeyR?url=http://www.thepeninsulaqatar.com/middle-east/140720-dozens-detained-in-saudi-over-flood-protests.html

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, Vol. 35 (1): 5-29

Risse, T. (2000). "Let's Argue!": Communicative Action in World Politics. *International Organization*, Vol. 54, No. 1 (Winter, 2000), pp. 1-39.

Robb, D. (2014). Sony Hack: A Timeline. Deadline: https://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/

Roberts, D. (2015). Obama imposes new sanctions against North Korea in response to Sony hack. *The Guardian*: https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview

Robertson, J. and Arnold, L. (2018). Cyberwar: How Nations Attack Without Bullets Or Bombs. Bloomberg: https://www.bloomberg.com/news/articles/2018-05-11/cyberwar-how-nations-attack-without-bullets-or-bombs-quicktake

Romo, V. (2019). Saudi Arabia Rejects Calls For Independent Investigation Into Khashoggi Killing. *NPR.org*: https://text.npr.org/s.php?sId=703590542

Saalman, L. (2017). New domains of crossover and concern in cyberspace. Stockholm International Peace Research Institute: https://www.sipri.org/commentary/topical-backgrounder/2017/new-domains-crossover-and-concern-cyberspace

Sanger, D. E.; Wong, E.; Erlanger, S.; Shcmitt, E. (2019). U.S. issues new sanctions as Iran warns it will step back from nuclear deal. The New York Times: https://www.nytimes.com/2019/05/08/us/politics/iran-nuclear-deal.html

Saudi Aramco's Facebook page: https://www.facebook.com/Saramcopage

Sayer, A. (1992). *Method in social science: A realist approach*, (2nd edition), Routledge.

Sayer, A. (2000). *Realism and social science*. Sage Publications.

Schwartz, M. J. (2016). Bangladesh Bank Attackers Hacked SWIFT Software. *Bank Info Security*: https://www.bankinfosecurity.com/bangladesh-bank-attackers-hacked-swift-software-a-9061

Seal, M. (2015). An Exclusive Look at Sony's Hacking Saga. *Vanity Fair*: http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg

Shamsi, J. A.; Zeadally, S.; Sheikh, F. and Flowers, A. (2016). Attribution in cyberspace: techniques and legal implications. Security Comm. Networks2016;9:2886–2900: https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1485

Shubber, K. and Sevastopulo, D. (2018). US accuses North Korea over global cyber crime wave. *The Financial Times*: https://www.ft.com/content/91453da8-b1de-11e8-99ca-68cf89602132

Siddique, H. (2015). North Korea responds with fury to US sanctions over Sony Pictures hack. *The Guardian*: https://www.theguardian.com/world/2015/jan/04/north-korea-fury-us-sanctions-sony

Smith, S. and Jovanovski, K. (2018). Turkish forensic teams search Saudi consulate for clues on Jamal Khashoggi. *NBC News*: https://www.nbcnews.com/news/world/turkish-forensic-teams-search-saudi-consulate-clues-jamal-khashoggi-n921491

Springer, P. J. (2017). *Encyclopedia of Cyber Warfare*. ABC-CLIO, LLC.

Steiger, S.; Harnisch, S.; Zettl, K. and Lohmann, J. (2018). Conceptualising conflicts in cyberspace. *Journal of Cyber Policy*, 3:1, pp. 77-95.

Sullivan, C. (2016). The 2014 Sony Hack and the Role of International Law. *Journal of National Security - Law & Policy*, Vol. 8 No. 3.

Tanter, R. (1998). *Rogues Regimes: Terrorism and Proliferation*, St. Martin's Press.

Tamkin, E. (2019). For first time, Saudi Arabia rebuked at the UN Human Rights Council. *The Washington Post:* https://www.washingtonpost.com/world/2019/03/07/first-time-un-human-rights-council-rebukes-saudi-arabia/?utm_term=.86a4d91954a4

The Department of Defense Joint Publication 3.0 Joint Operations September 17, 2006 Incorporating Change 2 (22 March 2010): https://www.bits.de/NRANEU/others/jp-doctrine/jp3_0%2810%29.pdf

The White House (2 January 2015). Statement by the Press Secretary on the Executive Order Entitled “Imposing Additional Sanctions with Respect to North Korea”: https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s

The White House, The Council of Economic Advisers (February 2018). The Cost of Malicious Cyber Activity to the U.S. Economy: https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Transcript of interview between Lakshmi Singh and Eric Swalwell (17 November 2018). Reports: CIA Concludes Saudi Crown Prince Ordered Killing Of Jamal Khashoggi. *NPR.org*: https://www.npr.org/2018/11/17/668953493/reports-cia-concludes-saudi-crown-prince-ordered-killing-of-jamal-khashoggi?t=1558090442295

Trew, B. (2018). Bee stung: Was Jamal Khashoggi the first casualty in a Saudi cyberwar? *The Indipendent*: https://www.independent.co.uk/news/world/middle-east/jamal-khashoggi-saudi-arabia-cyberwar-trolls-bee-army-missing-journalist-turkey-us-a8591051.html

Turner, A. (2019). State Department report calls Jamal Khashoggi’s death a human rights violation but doesn’t implicate the crown prince, Mohammed bin Salman. *CNBC*: https://www.cnbc.com/2019/03/13/state-department-calls-jamal-khashoggis-death-human-rights-violation.html

Tuysuz, G. (2018). Turkish officials raced to intercept Saudi plane after suspecting Jamal Khashoggi had been killed. *CNN*: https://edition.cnn.com/2018/10/19/middleeast/turkey-khashoggi-intel-intl/index.html

United Nations Counter-Terrorism Executive Directorate (January 2005). Frequently asked questions about UN efforts to combat terrorism: https://www.un.org/News/dh/infocus/terrorism/CTED_FAQs.pdf

United Nations Human Rights Office of the High Commissioner (25 January 2019). Independent human rights expert to visit Turkey to launch international inquiry into Khashoggi case: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24113&LangID=E

United Nations General Assembly Security Council (27 June 2014). Letter dated 27 June 2014 from the Permanent Representative of the Democratic People's Republic of Korea to the United Nations addressed to the Secretary-General: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2014_451.pdf

United Nations Human Rights Office of the High Commissioner (7 February 2019). Turkey: UN expert delivers early findings in Khashoggi probe: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24146&LangID=E

United Nations Human Rights Office of the High Commissioner (25 January 2019). Independent human rights expert to visit Turkey to launch international inquiry into Khashoggi case: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24113&LangID=E

U.S. Department of Homeland Security. Cyber Threat Source Descriptions: https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions#hack

Valeriano, B. and Maness, R. C. (2015). *Cyber War versus Cyber Realities – Cyber conflict in the international system*. Oxford University Press.

Vasquez, J. and Leskiw, C. S. (2001). The Origins and War-proneness of International Rivalries. *Annual Review of Political Science 4: 295-316.*

Wagner, W.; Werner, W.; Onderco, M. (Eds.) (2014). *Deviance in International Relations - 'Rogue States' and International Security*. Palgrave Studies in International Relations, Palgrave Macmillan.

Wang, C. and Kemp, T. (2018). CIA reportedly determines Saudi Crown Prince Mohammed bin Salman ordered the killing of Jamal Khashoggi. *CNBC*: https://www.cnbc.com/2018/11/16/cia-reportedly-determines-saudi-crown-prince-ordered-khashoggis-death.html

Weise, E.; Johnson, K.; Mandell, A. (2014). Obama: Sony 'did the wrong thing' when it pulled movie. *USA Today*: https://eu.usatoday.com/story/news/2014/12/19/sony-the-interview-hackers-gop/20635449/

Wheeler, T. (2018). In cyberwar, there are no rules. *Foreign Policy*: https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/

Yin, R. K. (2013). *Case Study Research: Designs and Methods (5th ed.*). Sage Publishers.

Young, A. and Yung, M. (1996). Cryptovirology: extortion-based security threats and countermeasures. *Proceedings 1996 IEEE Symposium on Security and Privacy*. Oakland, pp. 129-140.

Zetter, K. (2016). That insane, $81m Bangladesh Bank heist? Here's what we know. *Wired*: https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/