Swedish Defence University

Weaponized malware, physical damage, zero casualties – what informal norms are emerging in targeted state sponsored cyber-attacks?

The dynamics beyond causation: an interpretivist-constructivist analysis of the US media discourse regarding offensive cyber operations and cyber weapons between 2010 and 2020

Margarita Sallinen

Thesis, 30 ECTS (hp)
War Studies
Master's Programme in Politics and War
Autumn 2020
Supervisor: Jenny Hedström
Word count: 17968

Abstract

In 2010, the discovery of the malicious computer worm Stuxnet shocked the world by its sophistication and unpredictability. Stuxnet was deemed as the world's first cyber weapon and started discussions concerning offensive cyber operations – often called "cyber warfare" – globally. Due to Stuxnet, rapid digitalisation and evolving technology, it became vital for decision makers in the US to consider formal norms such as laws, agreements, and policy decisions regarding cyber security. Yet, to obtain a holistic understanding of cyber security, this thesis uses constructivism as its theoretical framework to understand changing informal norms and social factors including the ideas and morals of the US society regarding offensive cyber operations. This thesis critically analyses the discourse of three of the largest US newspapers by circulation: the New York Times, the Washington Post and The Wall Street Journal. A significant shift was discovered in the US media's publications and in informal norms regarding offensive cyber operations and the use of cyber weapons in just one decade, by comparing the discourses relating to Stuxnet in 2010 and the US presidential election in 2020. This thesis concludes that it is equally important to consider ideas and morals when researching a technical field such as cyber security by arguing that informal norms guide the choices actors make when developing formal norms at the international level. The findings of this thesis are intended to provoke a normative, urgent, and focused discussion about cyber security. The findings are also intended to shift attention to how language is used in discussions about the cyber sphere, offensive cyber operations and cyber weapons as components of the traditional battlefield.

Key words: constructivism, critical discourse analysis, cyber operations, cyber security, cyber warfare, cyber weapons, interpretivism, informal norms, media, war studies

Acknowledgements

I wish to extend my deepest gratitude to my supervisor Dr. Jenny Hedström for her helpful contributions and guidance throughout the writing process. I would also like to express my sincerest gratitude to Assistant Professor of War Studies Kristin Ljungkvist and Associate Professor Ilmari Käihkö for their helpful advice and practical suggestions.

I wish to also gratefully acknowledge the help I received from Dr. Lars Nicander, the head of Center for Asymmetric Threat Studies (CATS) at the Swedish Defence University, for his constructive criticism, encouragement and invaluable insight into cyber security.

I am also very grateful to my mother Larisa Sallinen for giving me the opportunity to study this master's degree. Lastly, I want to thank my loving fiancé Michael Daw for his profound belief in my work and who supported me throughout this entire process.

Table of Contents

1 Introduction

In 2010, Iran's uranium enrichment facility at Natanz suffered from malfunctions that caused hundreds of the centrifuges to spin and burn out. The controls failed to signal to the scientists of the substantial damage sustained by the centrifuges. The damage inflicted was caused by one of the most prominent malwares known at the time called Stuxnet – a targeted weaponized malicious software. While the incident resulted in no casualties, Stuxnet inflicted significant physical damage to Iran's nuclear facility and its nuclear program (Dunn-Cavelty, 2019, p. 420).

It was concluded that the cyber-attack was state-sponsored due to the sophistication and aggressiveness of Stuxnet. However, no official statement has ever been made and it seems plausible that the state(s) involved in this attack was either the US or Israel, or both (Lindsay, 2013, pp. 365-366). The sophistication of Stuxnet changed the perception of cyber-attacks in the global arena from being a mere abstract threat online to a digital threat that can inflict tangible destruction. A new definition was coined following the Stuxnet incident: *cyber weapon* (Farwell & Rhozinski, 2011, p. 31).

Stuxnet was called the "the Hiroshima of Cyber War" (Madrigal, 2011) that opened "the pandoras box of cyber warfare" (Chon, 2016), which ignited a fervent debate about whether the incident at Natanz was the genesis of "cyber warfare". Since Stuxnet, international discussions on cyber security have "exploded", and now constitute a key topic on national security (Dunn-Cavelty, 2019, p. 420; Russell, 2014, pp. 1-3). Cyber security experts have since begun to speculate about a new cybersecurity Revolution in Military Affairs – RMA - some experts even argue the cyber sphere now is an own war-fighting domain (Lindsay, 2013, p. 366). Further, technological developments have led to urgent discussions and the implementation of international laws and guidelines in the cyber sphere such as the Tallinn Manuals.

These examples suggest that the digital age has enabled elements of cyber activity, such as disinformation, cyber-espionage, and cyber-attacks being utilised in (and out) of conflicts in the modern world. This is supported by the fact that the creation of both Stuxnet and the term cyber weapon has resulted in a rapidly evolving and abstract threat landscape that comprises a cyber arms race (Dunn-Cavely, 2019, p. 424). Further, the US elections in 2016 and 2020 attracted more media attention on cyber security than ever before. It was even reported that both elections were investigated for falling victim to cyber-attacks, sometimes labelled as cyber warfare (Mello, 2020). The growing discourse on cyber security has also resulted in calls for an updated “digital Geneva Convention” that implements the cyber sphere into its framework and highlights the threat it may pose to humanitarian law (Guay & Rudnick, 2017).

Offensive cyber operations are, however, still considered a relatively new phenomenon that appears difficult to comprehend for many. This is mostly owed to its non-kinetic and kinetic nature, its disputed definitions and the vast amount of attention it has received over the past decade. Most information on cyber security is discoverable in policy documents, which provide strategies and recommendations on how to use networks and other technology to defend the state from cyber-attacks. These explanations are objective in nature and aligned with neo-positivist thinking, which examines causes and effects. However, to fully appreciate the complexity of cyber operations, it is essential to understand other dimensions such as informal norms like morals, social factors and changing ideas surrounding cyber sphere.

Hence, it is pertinent to explore how the informal norms surrounding cyber warfare have changed, especially since cyber space is now generally agreed to be a part of the battlefield (Broeders & van den Berg, 2020, p. 1). While formal norms in cyber security are constantly developing, there is a need to shift one´s thinking to the emerging informal norms and social relations since it affects the choices decision makers pursue in both the domestic and international arenas (Agius, 2019, p. 83). Herein lays the research puzzle: with rapid technological advancements and the ongoing development of formal norms in mind, how is the socially constructed reality, i.e., informal norms including ideas and morals, regarding cyber warfare changing in the US, and to what extent?

Offensive cyber operations concern cyber security – a very broad term which encompasses a variety of risks taken from different areas of the cyber sphere such as, for example, personal protection in the cyberspace to cyber-attacks on critical infrastructure (Carrapico & Barrinha, 2017, p. 1259). To create a more comprehensible understanding of cyber security, Dunn-Cavelty (2019, p. 413) divides the discourse surrounding this area into three discourses: (1) a technical discourse aimed at explaining malicious software – referred to as malware from here onwards, which includes worms and viruses; (2) a discourse surrounding crime-espionage, which concerns intelligence and counterintelligence; and (3) a discourse surrounding national security, critical infrastructure protection and matters often labelled as cyber war. Although the three discourses are highly interconnected, this thesis will focus on the third discourse, which concerns state sponsored cyber-attacks, offensive cyber operations, and cyber weapons.

Most contemporary research regarding cyber security and cyber operations focus on either the technological aspects or policy, which focuses on the implications cyber-attacks has or had for national security. A clear research gap exists in the literature on cyber operations regarding informal norms and socially constructed reality, i.e., normative factors are prioritized less in the pursuit of understanding the complex and abstract area of cyber operations. It is important that a balanced contemporary discussion about cyber operations is conducted where scholars from different research paradigms can share their ideas and work towards a more holistic understanding.

In addition, this thesis strives to generate greater understanding of the informal norms of the cyber sphere in the US. It encourages researchers and policy makers to prioritise understanding how quickly informal norms are changing, the impact this has on future cyber operations and policy making, and how it is viewed by the average American. Finally, this thesis highlights the importance of understanding the informal norms of one's own country and the impact this has on the concept of identity (Agius, 2019, p. 77). Further, it encourages one to develop awareness of international relations and of the common international norms regarding these questions to better understand how to build sufficient counter measures to cyber-attacks.

1.1 Key words

This thesis uses many key terms that have no universal definition. Defining terms in war studies presents a significant challenge that adds to the complexity of the overall discourse on cyber security. To answer the research question while mitigating the risk of ambiguity, the terminology and concepts contained in this thesis will be clarified.

Regarding constructivism, *informal norms* are often seen as the underlying guidelines of society (Risjord, 2014, p. 152). Collins (2019, p. 458) defines informal norms as "… the moral and ethical dimensions of international affairs, such as rules, beliefs and ideas". *Ideas* are thoughts, notions, and shared understandings, while moral norms, referred to here as *morals*, concern what is considered to be right or wrong conduct. (Risjord, 2014, p. 152). These two concepts are vital for creating and changing *identity* (Agius, 2019, p. 78).

It is also necessary to critically discuss the terminology surrounding cyber security. Numerous terms are used interchangeably by academics, policy makers and the media, including cyber war, cyber warfare, cyber operations and cyber-attacks. Many questions arise from this ambiguity which further adds to the abstract nature of cyber security – do these *concepts really exist*, what is their meaning and how are they perceived (Öberg & Sollenberg, 2011, p. 61)? Attempts at answering such questions have been submitted by individuals from a multitude of fields but without achieving universal consensus. For this reason, the definitions remain for the most part subjective (Andress, & Winterfeld, 2014, p. 4).

This thesis will adopt broad definitions as it is not the task of the author to conjure up narrow definitions in an interpretivist thesis. Nor will any attempt be made to postulate conclusive definitions as the author feels it is inappropriate to attempt such a task in a thesis conducting a discourse analysis. Yet, in order to answer the research question, the ideas of cyber warfare will be examined in light of 2010 and later in 2020.

To begin with, *Stuxnet* was the first known malware capable of causing physical destruction after it damaged the centrifuges at the nuclear facility in Natanz in 2010. Following this event, debates about *cyber war* and *cyber warfare* began. Since then, however, considerable confusion has developed regarding their definitions with both terms often being used interchangeably, despite possessing different meanings. Cyber war, for example, can be defined as two states fighting one another solely with cyber weapons in cyber space (Dunn-Cavelty, 2019, p. 420).

Like with cyber *war*, there is no universal definition of cyber *warfare* either and the definition is frequently debated. The term cyber warfare is understood by many as sharing the same definition as cyber war. Yet, when taken in isolation, the meaning of the word *warfare* is different from *war*. For this reason, numerous authors apply definitions from the physical world to the virtual world. For example, Andress, & Winterfeld (2014, p. 4) adopt Clausewitz's (1832) definition on how to conduct warfare from the Napoleonic Wars in 1873 and apply this to cyber warfare.

The terms *cyber war* and *cyber warfare* are often used in “everyday speech” and used as a buzzword by Americans to label general cyber activities (Rid, 2013, p. ix). For this reason, to use the word ‘war’ for cyber operations is often considered as undermining its true value (Stone, 2013, p. 101). For example, not one cyber operation has been labelled as an armed attack thus failing to satisfy the traditional definition of war. Furthermore, there has never been a declaration of war in the cyber sphere which means, according to public international law, that cyber warfare has never formally occurred. This puts cyber operations in a *grey zone* – a constant state of “unpeace”, i.e., the state between war and peace observable in cyber space (Broeders & van den Berg, 2020, p. 12).

This thesis prefers the term *cyber operations* since cyber *warfare*, in accordance with public international law, requires a formal declaration. The author understands it is problematic to loosely use the term cyber warfare in an academic paper – as highlighted by debates in popular discussions. However, in order to answer the research question and acquire an understanding of the everyday American’s perspective, the words adopted and analysed in the media discourse will include cyber *war*, cyber *warfare* and cyber *weapon* – these words were selected as they are the typical vernacular used in the US when labelling cyber operations.

Offensive cyber(space) operations (from now on cyber operations) can be broadly defined as “missions intended to project power in and through cyberspace” (Joint Chiefs of Staff, 2018). Interestingly, since cyber espionage is carried out in secrecy with the goal of long-term gathering and with no actual desire to cause an effect, it is therefore not considered as a cyber operation (Uren, Hogeveen & Hansson, 2018).

Further, a *cyber(space)-attack* is a type of cyber operation, which the US military doctrine defines as “actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain […]” (Joint Chiefs of Staff, 2018).

Cyber weapon is a generally accepted term. However, the term is problematic since cyber weapons can be used both defensively and offensively (Uren, Hogeveen & Hanson, 2018). The lack of clarity surrounding the definition of cyber weapons is easily illustrated by the definition provided in *Tallinn Manual 2.0*:

> Cyber weapons are cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack (Schmitt & Vihul, 2017, p. 452).

Additionally, *targeted* state sponsored attacks will be examined, and it is critical to point out the difference between a targeted and random attack. To clarify, it is the *intent* that determines whether an attack is random or targeted (Cavelty-Dunn, 2019, pp. 418-420).

1.2 Research question and aim

The purpose of this thesis is to generate understanding about the changing informal norms, such as morals and ideas, surrounding cyber operations in the US. Using interpretivism as its research paradigm and utilizing constructivism as a theoretical framework, this thesis will add normative and socially constructed knowledge to existing (neo)positivist research. The application of interpretivism and constructivism is vital to one's understanding of cyber operations, emerging non-traditional uses of force and the "informal, emerging laws". This thesis will therefore attempt to answer the following research question: Given the discourse in US news media since Stuxnet, how have the informal norms regarding "cyber warfare" changed in the last ten years in the US?

The main actor in this thesis is the US news media and, in particular, three of its biggest newspapers by circulation: The New York Times, the Washington Post and Wall Street Journal. The newspapers are a platform for public discourse that incorporates the views of the political leadership and civil society specifically in 2010 and 2020. The US was chosen as the actor under investigation because the internet – a significant part of cyber security – was invented there. Furthermore, the US plays a leading role in the discussion on this topic and is where the discourse on cyber security originated in during the 1970's (Dunn-Cavelty, 2019, pp. 412-413).

The scope of the thesis is limited in focus on two years: 2010 and 2020. First, 2010 was chosen because Stuxnet was discovered that year and is considered a "turning point" in the cyber world. Second, 2020 was selected because it is of great interest to examine developments in the discourse in this area over a decade, especially while the US election occurred. The author of this thesis is aware that two presidents held office throughout this period, which likely impacted the discourse – Obama relevantly held office in 2010, while Trump held office in 2016 until 2020.

This thesis aims to understand how US society was and is thinking about cyber operations and cyber weapons, and if and how the informal norms surrounding it have changed. To fully comprehend this, one should look beyond the same approach that one has always subscribed to, such as analysing scientifically observable knowledge, which is most common in a technical field. Alternative perspectives ought to instead be included in this area of research, which this thesis aims to demonstrate by conducting a critical discourse analysis on news articles from the three different newspapers.

This thesis aims to offer new insights in the field of war studies and how cyber operations can be researched. Additionally, this thesis aims to push the importance in understanding cyber security with socially constructed knowledge and assist in developing the existing cyber security professional "skill gap" in non-technical disciplines, which is of current concern (Oltsik, 2020).

Importantly, this thesis is not a technical report on ciphers or malware, nor is it a technical report on what occurred during the Stuxnet-attack. It instead attempts to understand a normative perspective, the *ideas* about cyber space as part of a battlefield and provide insight into the *moral* considerations and limits that emerge from the use of cyber operations in the US, as opposed to answering technical questions with technical language, which is prominent in data science.

It is the author's aspiration that professionals and scholars of technical fields alike can appreciate a non-traditional way of viewing cyber security, which is often not covered within their discipline. In addition, it is equally important to appreciate international relations in the cyber security field when evaluating governments and the public´s understanding of it. It is also vital to understand the discourse generated about pressing topics in contemporary society and to be reflective of one´s own thoughts and therefore raise awareness about source criticism.

1.3 Limitations of the study

To further clarify the purpose of this thesis, it is important to articulate what it is not. This thesis does not attempt to assign responsibility to any state as the perpetrator of Stuxnet, nor any other cyber-attack mentioned. It is also acknowledged that due to the complexity and secrecy behind cyber-attacks, the aggressor's identity is normally unknown. For example, neither the US nor Israel have admitted to any involvement with Stuxnet, despite many arguing that current evidence suggests otherwise (Dunn-Cavelty, 2019, p. 420).

The author considers the issue of ascertaining the party responsible as irrelevant as this thesis aims to *understand* the US and the *ideas* surrounding cyber weapons to assist in identifying western norms surrounding cyber operations. Further, this thesis focuses on cyber operations labelled as "cyber warfare" and cyber weapons but not any other "cyber activities". Accordingly, this thesis will not discuss cyber espionage – beyond what is presented in *section 2* – or cybercrime as they are beyond the scope of the research question. It is, however, acknowledged that cybercrime can hypothetically be state sponsored, while cyber espionage generally is state sponsored (Greenberg, 2019b).

Additionally, this thesis is a part of one semester in a master´s degree, which means the time and scope for writing this thesis was limited. Due to the time constraints, the author chose to compile the US news media and the US political leadership and society, as one unit of analysis. The author acknowledges that this simplifies a complex society that comprises hundreds of millions of people who each have their own thoughts and perceptions. Furthermore, interpretivism contends that reality is perceived differently by different people. Due to the limited scope of this thesis, however, the US media and society will be used as one unit of analysis. Moreover, this thesis will not provide any history of the US or its international relations nor of the history of internet and interconnectedness.

Mentioned in *section 1.2*, further limitations are encountered when writing about cyber war and weapons due to the ambiguity that exists regarding the terminology. In addition, the author acknowledges that when examining the details surrounding Stuxnet, it is arguable that this event was, to some degree, not a cyber operation since there was no online activity in the later stages of the incident. Stuxnet was likely able to infect the computers there via an infected USB-drive transported by a human infiltrator into the “air gapped” computer network at the nuclear facility, which suggests that it was not connected to the internet (Farwell & Rhozinski, 2011, p. 34). In most academia and everyday speech, however, Stuxnet is labelled as a cyber-attack and the author will refer to it accordingly.

Another prominent limitation stems from the secrecy surrounding cyber operations and the lack of academic research which can thus be conducted on it. Nevertheless, it is the author’s opinion that a critical discourse analysis that includes open-source material, like newspaper articles, can still add significant value to the academic literature in this area. This is supported by the fact that researchers are still producing papers on this topic even though one decade has passed since the Stuxnet incident occurred. It also demonstrates the importance of cyber security in contemporary security and war studies, and that the research on cyber operations and the norms and morals surrounding them, should continue to be explored. This thesis aims to contribute to this body of research.

1.4 Disposition

This thesis presents past research in *section 2*, followed by the theoretical framework constructivism in *section 3*. The methodology is presented in *section 4* and presents both the research paradigm interpretivism and chosen the method, critical discourse analysis. *Section 4* also presents the material used and the method process in depth. In *section 5,* the empirical evidence is presented, which consists of 12 newspaper articles. Following this, the analysis and its results are presented in *section 6,* followed by the conclusions in *section 7* and a presentation of the discussion in *section 8*. Lastly, three suggestions for future research are presented in *section 9*.

2 Previous research

Previous research on cyber security and the cyber sphere as part of the battlefield is scarce compared to that of traditional warfare. As mentioned in *section 1,* Dunn-Cavelty (2019, p. 413) explains that cyber security can be divided into three discourses: (1) technical; (2); cybercrime and cyber espionage; and (3) national security and critical infrastructure.

2.1 Technical discourse

The technical discourse focuses on computer networks, computer hardware and data science. All three discourses contain elements from the technical discourse. A significant volume of academic research on the technical aspect exists that contributes both theoretical and practical knowledge. It is aimed mostly at the IT field, with most literature explaining how malware like computer worms and viruses work. There is also a vast amount of research compiled on the names and explanations of the different types of attacks such as ransomware, DDoS-attacks etc. (Dunn-Cavelty, 2019, p. 415).

In the context of cyber operations, the technical discourse explains the technicalities and coding behind cyber weapons and how they operate and to what effect. There is considerable research on Stuxnet due to it being a so-called *zero-day* attack – it was programmed to find previously unknown vulnerabilities. To the author's knowledge, there is academia, albeit limited, written solely on codes called *cyber weapons* in conjunction with the technical discourse in war studies such as, for example, Félegyházi, (2012). The contributions made to the cyber security field has been enormous, yet there is still no research – to the best of the author's knowledge – that touches upon informal norms specifically in relation to the technical discourse.

2.2 Cybercrime and cyber espionage

Past research on cybercrime is very prominent in relation to the technical discourse. Whereas past research on cyber espionage is primarily focused on its history and implications for foreign affairs and national security. In relation to cybercrime, Gragido & Pirc (2011) explore different attacks and strategies by criminal non-state actors, focusing on cybercrime statistics in their book "*Cybercrime and espionage – an analysis of subversive multisector threats*".

Further, espionage (human intelligence) is complex and, from a democratic point of view, produces a vast array of interesting questions regarding morality. To illustrate, non-state sponsored attacks such as cybercrime often have the goal of misappropriating money and is illegal. Whereas cyber espionage is generally accepted due to regulations and since the task of state-sponsored intelligence agencies is to gather information through covert operations, i.e., espionage. Most research on informal norms relating to US covert operations and foreign policy focuses on espionage and morals (see for example Treverton, 1988).

Despite the secrecy surrounding it, substantial literature exists on the strategy and moral thinking behind cyber espionage as it involves questions concerning foreign policy. One example is Omand & Pythian´s (2018) book *Principled Spying: The ethics of secret intelligence*, where the moral dilemmas espionage presents in cyber space are investigated. The authors explore the challenges of cyber espionage and label it as digital intelligence vis-à-vis the Just War tradition – a theory that contemplates morals in war (Walzer, 2016). However, there is very little previous research on changing morals in relation to US cyber security or how it has been perceived by US society over the past decade.

2.3 National security and critical infrastructure protection

2.3.1 Cyber war is real

The American ideas about cyber war relating to national security can be traced back to 1991 during the Gulf War where the physical battlefield was considered insufficient. In contrast, a so-called "information dominance" was a deciding component for achieving victory in this war. However, the term cyber war was not widely used until 2007 following Russia's attack on Estonia's networks. This event is commonly agreed to be the first state sponsored cyber-attack, since the term cyber war was taken from theory and put into practice. After this incident occurred, the discourse concerning a "cyber war" taking place began to build momentum globally (Cavely-Dunn, 2019, p. 418).

Significant research published over the past decade exists on national security and critical infrastructure protection in the field of cyber security. However, there is considerable ambiguity in this research regarding the use of the word cyber warfare and its meaning (Angstrom & Widén, 2015, p. 107; Ranger, 2018; Stone, 2013, p. 107). Numerous authors argue that the cyber sphere should be considered as a war fighting domain equivalent to land, sea, air and space. This view was adopted in the book *Cyber Warfare: Techniques, Tactic and Tools for Security Practitioners* by Andress, & Winterfeld, (2014). On the one hand, the authors problematise the definition of cyber warfare. Yet, on the other hand, they maintain a declarative standpoint that cyber warfare is indeed occurring.

While the authors acknowledge that land, sea and air are the traditional warfighting domains, they argue that the technological and digital developments of the 21st century have resulted in modern warfare adopting two new domains: space and cyber space (Andress, & Winterfeld, 2014, pp. 41-42). They also argue after contemplating the classical literature on war studies, that the term cyber warfare can be traced back to the Napoleonic Wars in 1873. For example, they argue it is feasible to apply rational thinking about the historical concept of warfare to cyber warfare, such as that composed by Carl von Clausewitz (Andress, & Winterfeld, 2014, p.4). In his work "On War", Clausewitz (1832, p. 44) defines 'war' as "the continuation of politics by other means", which from the perspective of Andress & Winterfeld (2014, p. 4) is applicable to cyber war.

Interestingly, the authors mention that many US citizens likely hold the attitude that the last time the US was officially at war was WWII which, if true, suggests a cyber war could not have occurred yet (Andress & Winterfeld, 2014, p. 16). Despite this, the authors strongly argue that once a problem reaches the level that it becomes an issue of national security, the discourse concerning it may begin to adopt the usage of the term war. For example, even though the US was conducting military operations in Iraq in 2003 without having made a formal declaration of war, it was still referred to as being part of the "War on Terrorism". It is therefore unsurprising such attitudes may develop toward a cyber war existing. In summary, the authors suggest that cyber war is the correct term to adopt, that cyber warfare is real and given the nature of previous and current cyber-attacks likely means we are in a cyber war akin to a cold war (Andress & Winterfeld, 2014, p. 16).

Further, most contemporary research on cyber warfare emerged in the last decade with most of the focus being on conducting case studies on previous attacks. For example, Russel (2014) conducted a comparative case study in his book called *Cyber Blockades*. Once again, the definition of cyber warfare is associated with classical thinkers as Russel defines warfare by appropriating Sun Tzu´s thoughts on war from "The Art of War" as "the art and science of fighting without fighting; of defeating an opponent without spilling their blood" (Russell, 2014, p. 9).

Russell examines cyber war and applies this definition in two case studies: Estonia (2007) and Georgia (2008). Russel's research follows a well-trodden path by focusing on rational thinking while conducting his analysis of cyber war. Rationalism focuses on power projection, that is, using "means to an end" and power. Russel (2014) explains how countries without the capabilities to have any influence in the cyber world are perceived: "[t]o be absent from these networks of information is to be absent from power" (p. 2).

Another author, Andy Greenberg – a very influential US writer on cyber threats and a journalist in the magazine Wired – wrote the internationally recognized book *Sandworm: A New Era of cyberwar and the hunt for kremlins most dangerous hackers* (2019). Greenberg's book also focuses on case studies and examines the Russian threat in cyberspace, while specifically focusing on the targeted attacks on the Ukrainian power grids in 2015. Greenberg's contribution to the cyber security field has been extremely influential in the way cyber is perceived by American society.

2.3.2 Cyber war is a metaphor

For every proponent of cyber warfare existing, there are just as many opponents. Countless authors do not consider cyber war as a "real" war by arguing that it fails to meet the standard of what a war is and traditionally viewed as (Libicki, 2012).

Rid´s (2013) book *Cyberwar will not take place* offers valuable insights into the discussions about the concept of cyber warfare. He argues that cyberwar is merely a metaphor since it has not yet occurred nor is it occurring now and writes that "it is highly unlikely that it will disturb our future" (Rid, 2013, p. xiv). In stark contrast to Andress & Winterfeld (2014), as mentioned in *section 2.3.1*, Rid (2013, pp. 1-5) argues that Clausewitz's (1932, p. 29, p. 44) definitions of war from "On War" are not applicable to the cyber sphere. Rid (2013, p. 1) contends, for example, that war is violent, whereas cyber-attacks are not and asserts that the outcome of war can be lethal, while a cyber attack is completely void of any lethality.

Rid also argues that the terminology in cyber security is unstructured and flawed. He maintains that the hype surrounding cyber warfare is an over exaggeration and that a cyber apocalypse will never transpire. Rid does mention that cyber space has created more peaceful opportunities for action. For example, human intelligence gathering can now be achieved through computer breaches, which negates the potential of physical harm to an intelligence agent (p. viii). However, Rid (2013) argues that the real threat in cyber space is espionage, sabotage, and subversion, and that such activities are categorically different to cyber war. Rid makes no mention of informal norms in the cyber sphere and thus fails to reflect on the public's perspective.

Dunn-Cavelty (2019) – who has contributed greatly to the understanding of cyber security in this thesis from her chapter *Cyber Security* in *Contemporary Security Studies* – argues in accordance with Rid (2013), that the most prominent threat in the cyber sphere today is espionage, and that the fear of unrestrained cyber conflict is an over-reaction. She disapproves the term cyber war and believes that it is improbable that a war will ever be fought solely in cyber space. Instead, the author stakes her own claim in the terminology debate by proposing a new definition for cyber warfare, namely cyber(ed) conflicts (p. 418).

Dunn-Cavelty (2019, p. 425) does not present any research on informal norms in the cyber space. The author does, however, advocate the importance and urgency of going beyond measurable effects and proposes research on specific contents and contexts to investigate underlying subjective processes of key actors globally. She highlights the imperativeness of research for understanding meaning-making and therefore the importance of uncovering the shared understanding of how to respond to the threats in cyber space. This is what this thesis attempts to do.

Additionally, it is interesting to evaluate the use of cyber weapons as a *part* of military operations that do meet the threshold of war. Somewhat unsurprisingly, the literature becomes more apparent here, with cyber weapons often being written about as being part of a hybrid war. There is also an abundance of contemporary research on hybrid warfare and the closely related concept of "grey zones", that cyber operations are often associated with (Banasik, 2016; Fitton, 2016).

Lastly, there is the question of cyber terrorism, which is directly related to the discourse in cyber security concerning national security and critical infrastructure. Nicander & Ranstorp (2004) conducted one of the first comprehensive studies on non-state actors in *Terrorism in the information age: new frontiers?* The authors consider the role of traditional terrorism in the context of the cyber sphere and consider whether cyber terrorism will be a threat in the future and how it might manifest itself. While the argument over the existence of cyber warfare rages on, opponents and proponents alike can hopefully agree that one component of war in the digital age will at the very least be cyber operations. Regardless, discussions will rage on while a myriad of topics remain unsettled.

2.4 Guidelines

For the sake of triangulation, the understanding of cyber warfare will also be informed via a guidelines-perspective (formal norms) (Dulić, 2011, p. 46). Regarding formal norms, there are two well-known and influential international guidelines in the cyber sphere. The first is *the Tallin Manual on the international law applicable to cyber warfare* (Schmitt, 2013), also called Tallin Manual 1.0, which was developed by NATO in response to a Russian cyberattack on Estonia in 2007. Tallinn Manual 1.0 refers to fighting wars in cyberspace while suggesting laws and guidelines applicable to armed conflict. However, since cyber-attacks occur outside of armed conflict, there was a need to update it to remove such loopholes.

Accordingly, *the Tallin Manual on the international law applicable to cyber operations* (Schmitt & Vihul, 2017), called Tallinn Manual 2.0, was developed. As the titles suggests, the updated Manual was intended to cover a broader spectrum of cyber incidents in and *out* of armed conflict. Yet despite being accepted in the discourse for national security and critical infrastructure protection, Manual 2.0. has also received criticism, due in part to the ambiguity raised by the terminology and its applicability. The difficulty in its applicability is related to discussions regarding "*Jus ad Bellum*" – criteria that gives a state the right to conduct warfare. From a legal perspective, it is not "warfare" if it is not formally declared, as mentioned in *section 2.3.1*. Therefore, from the perspective of public international law, cyber operations remain in a grey zone.

In conjunction with previous research, Mazanec (2015) utilises norm evolution theory to predict how international law might evolve regarding cyber war in his book *The Evolution of*

Cyber War: International Norms for emerging technology weapons from a US perspective. His research is based on previous studies on the development of formal norms in relation to case studies on chemical, biological, and nuclear weapons, for example, and how they have changed, and then applies it to cyber warfare and cyber weapons. The author discusses numerous attacks and recommends the implementation of formal norms to limit them, while once again making no mention of informal norms (Mazanec, 2015, pp. 208-218).

2.5 Summary previous research

Research on cyber security generally focuses on technical, legal, policy and industry matters. The literature tends to disregard how informal norms develop and change over time. There is a clear research gap concerning cyber warfare, cyber weapons, and the study of understanding social factors like informal norms, and how they affect cyber and vice versa. This thesis aims to contribute to resolving this gap. Additionally, the author acknowledges that there is currently no universal definition for cyber war, cyber, war or warfare and that the authors who have conducted research on this topic have envisaged these terms differently. There are also many opponents and proponents for cyber warfare existing. (Angstrom & Widén, 2015, p. 107). Furthermore, there seems to be confusion over how to use the relevant terms due to the lack of universal definitions. Consequently, the concepts of cyber war and cyber warfare tend to be used interchangeably.

Currently, no cyber-attack has triggered a declaration of war by being present in cyber space. In addition, cyber warfare does not involve violence, which according to Clausewitz (1832, p.27) is a pre-requisite for something to be considered as war. (Rid, 2013, p. 1). When the updated Tallin Manual 2.0 (Schmitt & Vihul, 2017) was published, the term *cyber warfare* was amended to *cyber operations* to ensure guidelines concerning cyber-attacks outside of conflict were incorporated too. However, the problem remains in there being no formal declaration of war in cyber space. The updated Manual does, however, demonstrate the importance of changes in the language and understanding of the cyber sphere and its formal norms.

The author of this thesis once more wishes to clarify that her stance lays in the problematisation of using the term cyber warfare and prefers to refer to it as cyber operations. The author is also aware that this could contribute to differences of opinion with individuals that argue it should be called cyber warfare. Regardless of whether one thinks that the cyber sphere is the fifth warfighting domain or not, the research question can still be answered as the interest lays in the informal norms and the discourse surrounding the concept. That is, the perception of the US and the way its citizens think about the issue and whether they have or have not changed over the last decade, and if they have, then how.

3 Theory

3.1 Constructivism

Constructivism stresses the importance of understanding informal norms including morals, ideas and identities, when trying to comprehend international relations and security (Agius, 2019, p. 78, Wendt, 1999, p. 21). It focuses on the importance of ideational factors instead of material factors. It is arguable that the genesis of constructivism and its core concepts come from the sociological and philosophical thoughts of Immanuel Kant (Agius, 2019, p. 76). Kant, like many constructivist scholars, argues that knowledge cannot be objective since humans possess their own structures of understanding and common agreements about the meaning of things. Such thoughts continue to be relevant today, especially after Nicholas Onuf first coined the term constructivism in 1989. Constructivism has seen wide usage since and has reshaped the debate regarding rationalism being the dominant theory for understanding the world (Agius, 2019, p. 75).

A vast amount of academic literature on constructivism exists today. The most influential and well-known political theorist in constructivism is arguably Alexander Wendt, who is primarily associated with the concept of anarchy (Wendt, 1992; 1999). Erik Ringmar (1996) has produced literature on constructivism that relates to war studies, titled *Identity, Interest and Action, a cultural explanation of Sweden´s intervention in the Thirty Years War*. He uses constructivism to explain Sweden´s role in the 30-year-old war. Ringmar highlights that ideas and shared culture provide a better argument than the more classical or orthodox, i.e., rational explanations, which, according to Ringmar (1996, p. 145), fail to provide a comprehensive explanation.

Constructivism contributes to this body of research by highlighting the importance of underlying social factors, which must be understood since they guide actors and their decision-making. Hence, factors such as ideas, moral and identity are essential to consider since they play a significant role in an actor’s decision-making (Angstrom & Widén, 2015, p. 17). Constructivism still considers material factors such as economy, land and military power, important. However, material factors are interpreted through examination of social structures (Hurd, 2008, p. 4).

Constructivism argues that reality consists of social rules and the world is comprised of social systems. Individuals construct their own realities. Ideas, norms, rules are critical to understand as they inform how a state will act. Language and discourse also play a significant role in constructivism as language is the lens through which humans express and see their reality. Boréus & Bergström (2017, p. 9) explain the relation between constructivism and discourse as "our minds create, through language, ways of seeing the world".

3.2 Five key features of constructivism

First, there is no fixed, objective world, but reality is constructed through *social action* and the individual's perception of the world. Every individual participates in social construction, and not just those in a power position (Agius, 2019, p. 75, 79). Second, identities are constructed from the collective ideas of people, since shared ideas and interaction with others constitute how people understand the world (Agius, 2019, p. 78). Third, material power is not the only thing of importance, ideational structures matter too (Hurd, 2008, p. 4).

Informal norms are subjected to change as new forms of ideas can emerge, for example, which provides actors with the impetus to alter their shared understandings of a specific social phenomena (Agius, 2019, p. 83). This suggests that informal norms change over time. Last, pre-existing beliefs and expectations are an important part of what people base their social behaviour on while participating in social construction (Agius, 2019, pp. 79-78).

4 Methodology

The methodology section contains high levels of abstraction and it is important to appreciate the philosophical foundation that this thesis emerges from. Later, the method critical discourse analysis will be presented, and which material was chosen and how it was processed and evaluated.

4.1 Interpretivism

The research approach for this thesis derives from the interpretivist research paradigm. Interpretivist research is normative since it argues that there is no discoverable objective truth and is based on the researcher´s interpretation and "focuses on specific, situated meanings and meaning-making practices of actors in a given context" (Schwartz-Shea & Yanow, 2012, p. 2). This suggests that the author of this thesis has contemplated the concept of reflexivity, and acknowledges she is in focus and needs to detail her own possible biases, elaborated upon in *section 4.5*.

The epistemological assumption in the interpretivist research paradigm is that knowledge is socially constructed, and the ontological assumption is that the world is socially constructed too (Risjord, 2014, p. 6). In contrast to interpretivist academics, scholars of the (neo)positivist research paradigm follow the epistemological assumption that there is only one truth out there that can be measured. In addition, interpretive research does not test a hypothesis like (neo)positivism, and this thesis will therefore not contain a clearly written out hypothesis to answer (Schwartz-Shea & Yanow, 2012, p. 1, 53).

It is, however, important to continue and use an interpretivist research paradigm in war studies as it contributes to examining real-world problems through an alternate lens that stimulates the debate of important questions, which in this case concerns cyber security and underlying norms. The importance of interpretivism in war studies is demonstrated by, for example, Tannenwald´s (1999) article "The nuclear taboo". In this article, the author unveils how underlying social factors and norms played a significant role in the non-use of nuclear weapons, while rejecting the ethos that deterrence alone – a rationalist explanation – provides a complete answer.

4.2 Method

4.2.1 Critical discourse analysis

This thesis will use an intertextual approach, namely a discourse analysis. A discourse analysis is a qualitative and interpretive method that can be conducted in a multitude of ways. However, all approaches are perceived as a “study of language in use” (Gee, 2011, p. 8). One method of conducting a discourse analysis is to perform a descriptive discourse analysis which focuses on the linguistics used by closely investigating grammar, sentence structure and style of language.

Another well-known way of conducting a discourse analysis is to perform a critical discourse analysis, referred to from now on as “CDA” – a method often related to Fairclough (1992, 2010). Although a CDA is often approached in different ways, this thesis is inspired by Fairclough who divides the CDA into a three-dimensional model that comprises *text*, *discursive* and *social practice* (Dunn & Neumann, 2016, p. 36). This thesis will focus primarily on the first dimension *text*, since the aim is to uncover which discourses are found and articulated. Additionally, the third dimension *social practice* is partly mentioned since it is interrelated with the key points of constructivism whilst examining the effects the discourse on cyber operations has on social practice in the US, and vice versa. Although interrelated, the second dimension *discursive practice* – the production and consumption process – is outside the scope of this thesis and will not be touched upon.

The difference with the descriptive discourse analysis is that the CDA intervenes in political and social issues like cyber security. Critically, the CDA sees discourse not only as constituting, but as *constitutive* also. This means the discourse not only (re)shapes social practices, structures and processes but mirrors the societal structures and processes present as well. Boréus & Bergström (2017, p. 238) explain that a CDA “strongly emphasizes the importance of language and social relations are revealed through language”.

This thesis will thus focus on how the content and the theme “cyber warfare” is discussed by mass media in the US by critically analysing the discourse in its newspaper articles. CDA can be conducted on large volumes of different sorts of materials and small volumes of the same sorts of materials. In accordance with a CDA, most of the focus will be on how cyber warfare is presented and how the US is perceived in relation to power in society (Winther-Joergensen

& Philips, 2000, pp. 67-70). This should not be confused with a pure content analysis where the content is examined but not necessarily in the context of any specific time or theme.

The benefit of using a qualitative method in the field of cyber security, which is often perceived as technical, is that it examines underlying factors which cannot be quantified using mathematics. This thesis aims to understand how meaning around cyber warfare and cyber weapons is created through discourse from two different periods of time. Thus, a CDA complements the interpretivist paradigm and the constructivist theory which both focus on contextuality. Discourse is by itself a language and a way of labelling something observable, whereas a constructivist uses a discourse analysis to delve deeper and unveil the meaning behind the words used (Collins, 2019, p. 451).

A CDA was chosen for this thesis since it attempts to *understand* changing ideas and morals in the US. It also complements the theory of constructivism as informal norms and social change are examined with the context and time in mind. The reason why a CDA is chosen over a narrative analysis is because the focus is not solely on a single narrator. Instead, the research encompasses language used by numerous narrators discussing cyber warfare. As such, the ideas and morals presented within these discussions can then be identified from both time periods.

As with all methods, the qualitative method discourse analysis has its limitations. For example, it is dependent on the author´s interpretation, which is a common criticism made by (neo)positivist researchers regarding the testability of the results (Dunn & Neumann, 2016, p. 36). Another limitation is caused by time constraints and that the scope of this thesis is determined by the material used, which itself is limited to written material comprising a small sample of newspaper articles.

4.2.2 Choice of material

The CDA requires material that is appropriate to answer the research question. Mentioned above, due to time restraints for writing this thesis, the analysis will be applied to a small sample of material which focuses on US media and newspaper articles. Examining mass media is vital to cyber security and war studies, especially when the actor is a democracy like the US. After Stuxnet’s sophistication became apparent in 2010, the reporting on cyber-attacks has increased due to its relevance, negativity and continuity amongst other criterions considered for being newsworthy, resulting in significantly higher media attention (Öberg & Sollenberg, 2011, p.57).

Critically, when reading news in relation to cyber security it important to be mindful of what the media labels as cyber warfare since the goal of most political communication by actors through news media is to influence and establish power. Öberg & Sollenberg (2011, p. 60) state that actors attempt to use media outlets to try and acquire a positive view of themselves in relation to their "hostile" opponent, in order to gain political advantages from the outside world.

There are many reasons why mass media, specifically newspaper articles, are chosen for this analysis. One important reason is that it is informally called the fourth estate in the US because the public's opinion both influences and is influenced by what the media publishes. The US is also a democracy where information flows freely, which means that multiple news reports on a given story are comparable (Möller, 2011, p. 87).

4.2.3 Newspaper articles

Newspaper articles are an important source for understanding emerging informal norms regarding specific political questions. They can provide instant coverage of events as they occur, which is of great benefit to the researcher. Despite this, newspaper articles are often viewed as secondary sources unless the journalist themself has taken part in the event being reported on. The newspaper articles in this thesis are, however, seen as primary sources. The distinction between primary and secondary sources is often fluid since it is determined by the approach the author of a thesis takes when using the material. The reason the articles used in this thesis are primary sources is because they are being used to *understand* societal change and how the American society *perceives* cyber warfare, as opposed to trying to *establish knowledge about the actual events* (Dulić, 2011, p. 36; Möller, 2011, p. 76).

Additionally, it is important to include a variety of news sources to mitigate the risk of potential bias in the research and to obtain a richer "pool of information" (Möller, 2011, p. 87). Accordingly, three newspapers owned by three different companies were chosen. It is also worth mentioning that the media reports on what it believes its subscribers want to read. Thus, one must keep in mind that the newspapers in this thesis do not provide the full picture of the events that unfolded (Möller, 2011, p. 76). Source criticism is also important and despite journalists calling themselves neutral, one must consider all the information acquired through a criticizing filter. To accomplish the goals of this thesis, however, three newspapers were chosen based on the quality of journalism, and especially since they strive for neutrality in what they report (Öberg & Sollenberg, 2011, p.49).

Since the discourse surrounding "cyber warfare" in the US media will be investigated, there is great value in examining several of the leading daily newspapers by circulation in the US. While placement in the top 10 daily newspapers differs from year-to-year, three newspapers have consistently placed highly in recent years, which suggests that they are amongst the most trustworthy daily newspapers (Cision Media Research, 2019). As such, the three chosen newspapers are: The New York Times, the Washington Post and the Wall Street Journal – all three will be examined in print and digital form. The author is aware that these newspapers are only available via subscription and orientate towards liberal/democrat values.

The limitation with using newspaper articles is that it is considered non-academic material like open-source material. Further, news articles are not neutral in their reporting and media in the US, for example, is part of an economic and political setting, which means that journalists will deliberately leave parts of a story unreported while emphasizing others (Möller, 2011, p. 83). Öberg & Sollenberg (2011, p. 72) highlight the importance of source criticism in peace and conflict studies and state that "information is part of warfare and news media is part of the battlefield". Biases in journalism can be both deliberate and unintentional, especially where a journalist lacks sufficient knowledge of a specific event (Dulić, 2011, p. 42).

Nevertheless, newspaper articles provide essential information for research on changing informal norms and the values of a given society. To help remove biases in the material used, the five principles of source criticism were considered while writing this thesis: authenticity, dependency, reliability, tendency, and time (Thurén, 2019, p. 12). The method of CDA fits the material perfectly too since open source is acceptable to use.

4.2.4 Data collection

First, the author chose to use the information and news service database Factiva (Möller, 2011, p. 79). Factiva is available at Stockholm University's library, to gain access to the empirics, the author had to use the database, as the newspapers are only available with subscription otherwise – note: Factiva can only be accessed by being physical present in the library, which the author was. The following search words were entered in the free text search square while searching the database: “Stuxnet *and* cyber war *or* cyberwar *or* cyber warfare *or* cyberwarfare *or* cyber weapon *or* cyberweapon”. This was necessary to narrow the hits as the terms entered after Stuxnet are frequently written differently and often with or without spacing (Öberg & Sollenberg, 2011, p. 72).

Dates were also entered to narrow the period to between 1 August 2010 and 31 December 2010. Thus, a time span of five months was selected as a filter as despite Stuxnet being discovered in June 2010, it was not until August 2010 that it was determined that it had primarily affected Iran and that the damage to the centrifuges in Natanz was reported (Dunn-Cavelty, 2019, p. 420). Hence, the timeframe of interest is August 2010 to the end of 2010.

Second, region was chosen to focus on the United States since it is the chosen actor, and the language was automatically set to English. Once the search finished, the author sorted the newspaper articles *by relevance* to let the dataset determine what articles are most relevant and to attempt to acquire a random selection of articles rather than sorting the articles by date. Next, the source that was going to be examined was entered: the New York Times or NYTimes.com Feed was entered first, which gave 15 hits. The author read through each article one at a time and the articles that were not relevant to the research were disregarded, for example, letters to the editor and other types of articles that related only to a main article were not selected for analysis.

To obtain a simple overview of the headlines and the articles they belong to, the author entered “reference letters” in brackets next to the headlines. Important information about each article can be found in section *5*, *Table 1,* and *Table 2.* Of the 15 hits obtained from the search from the New York Times, headlines 1(A) and 2(B) were selected. The author then modified the search to The Washington Post or Washington Post.com, which gave 16 hits. From this, headlines 1(C) and 3(D) were selected. Lastly, the author modified the search to Wall Street Journal or The Wall Street Journal Online, which gave 14 hits. The headline 1(E) and headline 10(F) were selected.

The author followed the same procedure for 2020 albeit with several important changes. First, the author changed the timeframe to 10 June 2020 to 10 November 2020. Thus, the timeframe was deliberately kept to 5 months. This timespan was selected as the election was held on 3 November 2020 and because it is of interest to this research to examine whether there was any interference prior to the election taking place. The search words were also changed to include: Trump *and* election *and* cyber war *or* cyberwar *or* cyber warfare *or* cyberwarfare *or* cyber weapon *or* cyberweapon.

The process was otherwise the same as 2010, i.e., the sources entered were identical. There were 10 hits for New York Times, with headlines 3(G) and 10(H) being chosen. There were 16 hits for Washington Post, with headlines 1(I) and 2(J) being selected. There were 21 hits for Wall Street Journal, with headlines 1(K) and 12(L) being chosen. By this stage, the author had obtained all the material she needed and could progress to starting the CDA.

When starting the CDA, the author decided to conduct a so-called pilot study, where articles A and G were examined. This was performed to find the most appropriate way of conducting the CDA by highlighting what stands out most in the discourse regarding the research question, cyber warfare and weapons (Boréus & Bergström, 2017, p. 28). Additionally, it was important to identify whether the informal norms changed or remained constant. It was also of interest to see if and what new norms emerged and if they have changed and how, in relation to ideas and morals. Three techniques in CDA were kept in mind: (1) *modality* – how certain a journalist or actor expresses him/herself; (2) *normality* – if an issue is toned down; and (3) *transitivity* – how the issue is portrayed in relation to who is to blame, i.e., choice of perspective (Boréus & Bergström, 2017, p. 156).

This was accomplished by highlighting the *charged words* – words that are intended to provoke a reaction from the reader – and by thinking about how the US portrays itself in relation to other nations. For example, if there was any thinking akin to "us vs them" (polemics) and, most importantly, how cyber warfare is discussed, i.e., how the journalist(s) uses the words cyber war, cyber warfare or cyber weapons in the specific time and context. Lastly, the analysis attempted to unveil hidden meaning only discoverable by reading "between the lines", i.e., the underlying ideas and morals about what is *not* being said, such as what is "explicitly stated but implicitly understood" (Boréus & Bergström, 2017, p. 223). This analytical process was applied throughout the 12 articles and despite only analysing a small sample of newspaper articles, a very clear and peculiar pattern was observable.

Due to the many approaches with CDA, there is no clear or universal template to reply on for the analysis. Therefore, the author freely identified seven (7) overarching categories regarding informal norms in relation to changes in the discourse (Boréus & Bergström, 2017, p. 224; Nyberg & Tidström, 2012, pp. 135-136). The analysis and results in *section 4* will be presented by category for clarity, although being highly interrelated. The following four (4) categories were identified about *ideas* of cyber warfare in the analysis:

- Ideas about what cyber warfare is/how is it talked about?
- Ideas about what cyber weapons are
- Ideas about the objectives of cyber warfare
- Ideas about capabilities and future predictions

Further, in regard to *morals*, two (2) categories were identified:

- Morals regarding actors (the self vs others)
- Morals regarding retaliation

In addition, one (1) last category was identified regarding what is implicitly understood:

- Ideas and morals regarding what is *not* explicitly stated

4.3 Reflexivity

It is essential to consider reflexivity in an interpretivist thesis. This entails acknowledging who the author is and what may lead to bias being present in the research (Risjord, 2014, p. 62). The thesis is written from a western perspective and the chosen newspaper articles are considered liberal leaning. The researcher has a Russian/Finnish background, was born in Sweden and identifies herself as a westerner. However, her Russian background could potentially affect the analysis of a paper examining the US perspective. The author is also a student at the Swedish Defence University and naturally leans towards security thinking.

Interestingly, the author had limited knowledge about cybersecurity and the many complex issues surrounding the discourse on cyber warfare prior to writing this thesis and was primarily informed from what is written in digital news media. Despite this, however, the more research the author conducted, the more she was able to discuss contemporary issues with other practitioners in the field. From this, the author's perception and understanding of cyber security and the words cyber warfare, cyber war and cyber weapons has significantly changed. The author has found the overall process of understanding and the application of critical thinking of what cyber security is, who talks about it and in what way, most enlightening. All points mentioned above were consistently contemplated by the author throughout the entire research process.

5 Empirics

The empirical material in this thesis consists of 12 newspaper articles from the New York Times, The Washington Post and The Wall Street Journal. The articles have been labelled, first A-F (Table 1) and then G-L (Table 2). The reason for this is to eliminate the need to write out each article repeatedly. Table 3 presents the authors of each article to eliminate bias.

5.1 News articles 2010

Table 1

Newspaper articles regarding cyber war, - warfare and - weapons in 2010

Reference letter	Headline and date	Newspaper
A	A code for chaos *03/10/2010*	The New York Times
B	In a computer worm, a possible biblical clue *30/09/2010*	The New York Times
C	A destructive internet worm could be potent cyber weapon *19/12/2010*	Washington Post
D	Stuxnet malware is blueprint for computer attacks on U.S. [corrected 8 oct 2010) *02/10/2010*	Washington Post
E	How to fight and win the cyberwar *06/12/2010*	The Wall Street Journal Online
F	U.S. News: Cyber attacks test pentagon, allies and foes *25/09/2010*	The Wall Street Journal Online

Note. This table contains (in order): reference letter, title of news article, date it is written (dd/mm/yyyy) and from which newspaper.

5.2 News articles 2020

Table 2

Newspaper articles regarding cyber war, - warfare and - weapons from 2020

Reference letter	Headline and date	News paper
G	How will the U.S. combat election day cyberwarfare? With paper. *18/10/2020*	NYTimes.com Feed
H	Trump claims credit for 2018 cyberattack on Russia *11/07/2020*	NYTimes.com Feed
I	Overstating the foreign threat to elections poses its own risks, U.S. officials and experts say *30/10/2020*	Washington Post
J	Biden´s foreign policy theme: America´s back *22/10/2020*	Washington Post
K	Will we have a Cyberwar or Cyber Peace? Richard A. Clarke, a former White House counterterrorism and cybersecurity chief, offers two competing visions of 2030 *09/10/2020*	Wall Street Journal
L	U.S sanctions additional Iranian banks; move aims to sever few financial connections Teheran still has to world *08/10/2020*	Wall Street Journal

Note. This table contains (in order): reference letter, title of news article, date it is written (dd/mm/yyyy) and from which newspaper.

5.3 Authors of the news articles

Table 3

Authors of newspaper articles A-F (2010) from Table 1 and Table 2 G-L (2020)

Reference letter	**Author(s) newspaper articles 2010**
A	John Markoff
B	John Markoff, David E Sanger, William J Broad
C	William Maclean
D	Ellen Nakashima
E	Mortimer Zuckerman
F	Siobhan Gorman and Stephen Fidler
Reference letter	Author(s) newspaper articles 2020
G	Kassie Bracken and Alexandra Eaton
H	David E Sanger
I	Ellen Nakashima
J	Karen De Young
K	Richard A. Clarke
L	Ian Talley

6 Analysis and results

The following section will present the results of the CDA conducted on the 12 articles selected. This analysis links back to the constructivist theoretical framework, to assess where they align. This section is divided into three parts, first how the ideas and second, how the morals regarding *cyberwarfare* have changed 2010 compared with 2020.

6.1 Ideas

6.1.1 Cyber warfare

2010

The ideas revealed from the discourse in articles A-F is that cyber warfare was perceived as *fear-provoking*, revolutionary and threatening; a wake up-call for the beginning of a *new* era of warfare that no one is guaranteed protection from. Article F also goes as far as to compare it to nuclear weapons, which are generally agreed to have changed warfare following their invention. The idea was that cyberwarfare should be feared, which leaves the reader apprehensive about the effect it could have in the future – the discourse expresses the idea that cyber warfare is a novel form of war, described by charged words.

For example, in the title in article A, one is immediately confronted with charged words such as "code" and "chaos", and it is arguable that the journalist is convinced it is something to fear and wants to convey this message. Numerous charged words are also found in article B, including "weaponized", "attack", "age of cyberwar", which leaves the reader with an uncomfortable feeling about what might come next.

Further, the discourse in article C is bleak and fear-provoking as demonstrated by charged words such as "damage" and "all-out-conflict". The article's underlying message appears to be that there was no political or military preparedness compared with that of traditional warfare, and that there was therefore no psychological preparedness either. Article D also contains countless charged words in its headline and discourse including: "blueprint" together with "attacks". Fear is further demonstrated by the following quote: "it could be only a matter of time before similar threats show up here" (Maclean, 2010). Further, article F demonstrates a similar tone and *idea* about the seriousness and surprise-element of cyber warfare: "'Instead of messing with the nervous system, you´re going right to the brain now,' one U.S. official said." (Gorman & Fidler, 2010)

2020

In 2020, however, the perception of cyberwarfare being an ominous "surprise" is largely non-existent. It seems that cyberattacks are now tolerated and anticipated in everyday political life and there is a general understanding that cyber warfare is currently being utilised. This *normalisation* of cyber-attacks appears, at times, to downplay the seriousness that such attacks may present. This is observable in Article I, which focuses on the negative effects caused by *overstating* the danger that a cyberthreat poses to a nation: " 'My biggest concern is that we give a foreign adversary more credit than they´re actually due,' said Brig Gen. Joe Hartman, the election security lead for the military´s U.S cyber command […]" (Nakashima, 2020)

This discourse highlights the relaxed attitude cyberwarfare currently receives, and the mindset that overstating an adversary's cyber capabilities could harm a country more than an actual cyber-attack could. Further, in article G, the words *combat* and *cyberwarfare* are charged words but are, however, followed by the words *with paper* – article G promotes the idea that the American people should not feel concerned about cyberwarfare during this year's election since 95% of voters will use paper.

The soft tone used in article G while writing about cyberwarfare leaves the reader with the impression that cyberwarfare is not something to be concerned about. This is especially noticeable when compared to other articles written on traditional modes of warfare. This idea is clearly established in the article with statements such as: "[…] voters should feel more confident than ever in 2020. 'This will be the most secure election we´ve ever held,'" (Bracken & Eaton, 2020)

The result shows a significant change in the ideas about what cyber warfare is, which is aligned with the key points of constructivism. For example, norms and ideas can change over time and we base our understanding on pre-existing ideas, that is, cyber warfare is nothing "new" anymore and we are now desensitised to it. Further, it emphasizes the importance of the US striving to be perceived as having a strong and secure identity on the world stage. (Agius, 2019, p. 75-79). This aligns with CDA, where normalisation is used to downplay the seriousness of cyber warfare in 2020, and modality, the one giving the statements seems very certain of what they say, which further makes the statement trustworthy (Boréus & Bergström, 2017, p. 156).

6.1.2 Cyber weapons

2010

In 2010, the discourse about cyber weapons is present in all articles (A-F), while also being associated with Stuxnet. The idea is that cyber weapons are secretive, mysterious, and incredibly successful. For example, article A demonstrates the considerable secrecy surrounding Stuxnet and the idea that identifying its creator is improbable: "Most computer security specialists say the authorship or the program may never be discovered" (Markoff, 2010). Further, article B similarly discusses Stuxnet's secrecy: "In interviews in several countries, experts in both cyberwar and nuclear enrichment technology say the Stuxnet mystery may never be solved" (Markoff, Sanger & Broad, 2010). Akin to articles A-C, in article D, there is discourse concerning the secrecy of cyber weapons: "Researchers still do not know who created Stuxnet or why" (Nakashima, 2010).

The discourse on the idea that it was successful, ground-breaking, but distressing is demonstrated by articles C and D. While article C discusses Al Qaeda's potential to acquire weapons that can sabotage computers, it manages to draw a comparison with Stuxnet by describing it as something new and petrifying: "Stuxnet is like the arrival of an F.35 fighter jet on a World War I battlefield" (Maclean, 2010). Additionally, article D writes: "Stuxnet opened pandoras box" (Nakashima, 2010) and describes Stuxnet as the "malware of the century".

There is an underlying idea about Stuxnet, that its sophistication suggests that the US is not prepared for what will come next. The discourse concerning the use of malware like Stuxnet in cyberwarfare, aligns with the idea that responsibility can be difficult to determine due to the clandestine nature of such attacks and that malware, for example, can be used successfully in military operations (Dunn-Cavelty, 2019, p. 417). Therefore, it is arguable that the discourse in 2010 attempts to show that a pandoras box has opened, and that the use of cyber weapons has resulted in a new warfighting domain, the consequences of which are not yet known.

Stuxnet is emphasized as being powerful and modern, and the idea that Stuxnet was an incredibly successful attack is thus uncovered and that future attacks could result in much greater calamities. Article C's headline demonstrates this idea by using charged words like "destructive" and "potent cyber weapon", while article E also writes that: "It is the world´s first-known super cyberweapon designed specifically to destroy a real-world target" (Zuckerman, 2010). Further, the word cyber weapon was invented after Stuxnet, meaning an idea about what a cyber weapon is had not developed yet. Article D demonstrates the novelty of the concept, and that the term cyber weapon had not been used before: "What this is essentially a cyber weapon" (Nakashima, 2010),

2020

In 2020, the term *cyber weapons* is only mentioned in article K: "*Some nations have already loaded their cyber weapons*". The sentence uses entirely charged language, especially the words *loaded* and cyber *weapons*. However, there is no explanation of what cyber weapons mean. Since none of the other articles from 2020 mention cyber weapons the same calibre as Stuxnet, which in 2010 was the idea of what a cyber weapon is, the idea of cyber weapons is likely now associated with other cyber activities.

The results and confusion about what cyber weapons are can be linked to the issues of coherent terminology and diffuse definitions in cyber security – as mentioned in *section 1.2*. If a cyber weapon is used in a cyber war during 2020, does it mean cyber weapons are used in cyber espionage? It is also possible that the idea is that cyber weapons are not used, despite the act being called cyber war.

6.1.3 Objectives

2010

The discourse in 2010 unveils the idea that the objective of cyber warfare is destruction and or disruption of critical infrastructure, as agreed in articles A-F. This is not surprising since Stuxnet damaged physical infrastructure in Natanz, and the idea of the American population naturally leads to concerns of their own critical infrastructure.

The concern is that the current objective of cyber warfare has transitioned from the virtual realm to the physical world, the idea of which is demonstrated by article A that describes Stuxnet as "world-breaking": "Previously, most high-profile cyberattacks have focused on Web Sites and corporate or military networks" (Markoff, 2010). The idea that the target of cyber warfare is now critical infrastructure is also seen in article E: "Few nations have used computer networks as extensively as we have to control electric power grids, airlines, railroads, banking and military support" (Zuckerman, 2010).

2020

In comparison, there is no common understanding in 2020 on what cyber warfare's objective is. The discourses make no mention of malware like Stuxnet or its potential to cause physical damage. Article G, for example, concerns itself with the 2020 US election instead, and chooses to focus on the Russian *interference* in the 2016 US election and the lessons learnt from it: "The 2016 U.S. election was a game changer for voting technology. Widespread Russian interference in out voting systems spurred new federal scrutiny of the country´s vast and fragmented election infrastructure" (Bracken & Eaton, 18 Oct 2020).

This result indicates that the idea about the cyber warfare's objective in 2010 was to attack critical infrastructure – a targeted attack with considerable impact. Whereas the idea in 2020 appears linked to low-level incidents and cyber espionage (Dunn-Cavelty, 2019, p. 415).

6.1.4 Future predictions

2010

The discourse from the 2010 articles (A-F) differ only marginally from one another in regard to the ideas about future predictions on cyber warfare. The idea of the future of cyber warfare is portrayed as dark and uncertain, which can be seen in article D: "We don´t need to be concerned about Stuxnet, but about the next generation malware we will see after Stuxnet." (Nakashima, 2010). Articles C and F suggest the idea that non-state actors, such as terrorists, could acquire cyber weapons like Stuxnet. This leaves the reader with a glum impression; if terrorists can acquire such weapons then an attack could happen anytime, in any location and that anyone, including civilians, could be a victim. The idea is that the future could entail a potential catastrophe.

Second, the idea uncovered is that every nation should be concerned about protecting themselves. Article C proposes no hope in solving the issue of cyber warfare in the future and gives the impression it is an impossible task. This is reinforced by the following statement that suggests that even international cooperation cannot stop terrorists from acquiring cyber weapons: "Lagner says multinational efforts against malware inspired by Stuxnet won´t work because 'treaties won´t be countersigned by rouge nation states, terrorists, organized crime, and hackers." (Maclean, 2010).

2020

In contrast, the discourse in the 2020 articles (G-L) concerning future predictions and the capabilities of cyber warfare differ significantly from each other. It is arguable that these variances can be linked to the massive volumes of information on cyber security created in the last decade and the heightened media attention it now receives. Article K stands out and distinctively mentions future predictions. It presents *two opposing ideas* about cyber in the future in relation to AI (artificial intelligence). First, proposing a possible "cyber peace": "By 2030 such a network-defence and network-control master algorithm might greatly reduce cyber risks. Cyber peace might break out" (Clarke, 2020). This is one of the more interesting future predictions on cyber warfare, since it suggests it may contribute to peace.

Shortly after, however, a more alarming alternative is presented: "Alternatively, by 2030 we may have had our first cyberwar, a hyper-speed conflict involving widespread nation-state attacks on each other´s critical infrastructure, including telecommunications, pipelines, financial systems, and electric-power generation and transmission networks" (Clarke, 2020). The important word to acknowledge is "first" – article K sees cyberwar as something futuristic in 2020.

This is seen in the following quote too: "It there were to be a full-scale cyberwar, we could expect that many parts of the U.S. would be without networked electric power for months." (Clarke, 2020). It is interesting to emphasize the words "if there were to be" since it acknowledges the idea that cyber war *has not taken place yet* and disregards all attacks thus far as cyber warfare. Article K discusses cyberwar as nations attacking each other's critical infrastructure back and forth, which aligns with the definition of cyber war presented in *section 1.2*.

Further, article L is the only article selected from 2020 that portrays cyber warfare and future predictions in a chilling way. The article uses charged words that causes the reader to react by stirring up strong negative emotions: "But if Mr. Trump is re-elected, some experts expect simmering frictions could boil over, with regional proxy clashes and cyberwarfare escalating into direct military confrontation between the two nations and their allies" (Talley, 2020). The idea here is that future cyberwarfare can provoke traditional military action via escalation from cyberwar.

Further, the future predictions on cyber warfare and the idea of "every nation for themselves" in 2010 has now changed. Article J, highlights the idea about cyberwarfare as being a problem which should be tackled together with other nations, and the need and willingness for international conversation and acknowledgement of the power of cooperation in the cyber-security field: "'Climate change, nuclear proliferation, great power aggression, transnational terrorism, cyberwarfare, disruptive new technologies, mass migration – none of them can be resolved by the United States, or any nation, acting alone,' Biden said in the 2019 speech" (DeYoung, 22 oct 2020).

The ideas about future predictions in 2010 align with the previous research by Nicander & Ranstorp (2004), where the question arises about how it will look if non-state actors like terrorists use the cyber sphere to achieve their aim, and thus conduct cyber terrorism. It is further linked to constructivism, since there was no pre-existing belief about what cyberwar is, so the future is perceived as uncertain. This change in ideas about security collaboration in 2020 also aligns with constructivism, i.e., identities are not set-in stone and can change over time.

Agius (2019, p. 83) states that “actors alter their relationships and understandings, from potentially antagonistic to cooperative”. Although article J presents a quote from 2019, Biden states the idea about the US cooperative identity on the world stage, which sends a signal of “themselves” as strong, world leading and willing to take on important tasks such as peace resolution, meaning the new ideas create collaboration and new security communities (Agius, 2019, p. 83).

6.2 Morals

6.2.1 Actors – the Self and Others

2010

In 2010, the idea of being the creator of Stuxnet was considered immoral and uncivilized. The articles (A-F) all promote the idea that the US took on the identity as the potential victim whose morals prevent them from engaging in cyberwar, while pointing the finger at other nations like China, Russia, and Israel as the primary aggressors. Article B demonstrates the discourse regarding "the Self" as a victim: "No country, President Obama was warned even before he took office, is more vulnerable to cyberattack than the United States" (Markoff, Sanger & Broad, 2010).

Regarding "the Others", articles A, C and E specifically mention China, and articles B and C talk about Russia, while A, B and D discuss Israel as the suspected creators of Stuxnet. For example, as seen in article A: "China, Israel and the Palestinians are all known to have irregular cyber armies of motivated hackers with significant skills." (Markoff, 2010). North Korea is also mentioned in article C as an intercessor for acquiring cyber weapons.

The underlying, and perhaps hidden discourse regarding morals surrounding cyber warfare and any involvement in the creation of Stuxnet is that "this is not who we are", which expresses the *morals* that it is "impossible" the US would act this way and is directly tied to one's perception of their own *identity* and the undesirability of such conduct being associated with them demonstrated in article A: "But many military and intelligence analysts, including several with direct knowledge of Israeli intelligence operations, have said it is unlikely that either an Israeli or United States operation would leave such blatant clues." (Markoff, 2010).

Article B also emphasizes that the US is building its capacity to achieve a strong cyber security unit while also promoting the idea, similarly to article A, that the US is a victim in relation to Stuxnet. This strengthens the idea that the US wants to emit to the world that it would never commit such an immoral act – this is greatly concerned with *transitivity* and the discourse surrounding "us" and "them" (polemics).

2020

The discourse about how the US portray themselves in 2020 in relation to cyber warfare and the morals behind engaging in it has changed in an astonishing way. It is evident in article H that the morals behind being the threat actor in cyberwarfare has made a U-turn since 2010. While the original rhetoric in 2010 was “this is not who we are”, Trump blatantly declares in 2020 his own responsibility for a cyber-attack on Russia in 2018, which points to the idea that “this *is* who we are”.

It is arguable that this counts as retaliation to the Russian interference in the 2016 election: “The move was intended to deter Russians from interfering in the midterm elections and serve as a test of America´s capability to protect the 2020 elections” (Sanger, 2020). The identity and the way the US seek to portray itself has changed from wanting to be viewed as one of the victims in 2010 to now admitting it and possibly wanting to show off to be perceived as a leading force in cyber security. One way of looking at it is that the underlying meaning in article H, for example, is that it is morally more defendable than a traditional war. This is extremely interesting since article K mentions the idea of cyber peace instead of more conflict in the future.

Article H also avoids labelling cyber weapons as a “super-weapon like Stuxnet” as was the case in 2010, and instead labels cyber warfare as interference. It further downplays the Russian capabilities by labelling their cyber-attack on the Russian party responsible for the 2016 US election hack, as not being a complex operation, for example: “While not especially sophisticated – United States Cyber Command knocked the group offline for a few days around the 2018 midterm elections – it is often cited as a prime example of American cyberwarfare making use of new leeway […]” (Sanger, 2020)

The US tries to establish a form of authority on the geopolitical field and perhaps stabilising the international relations, which is uncovered while keeping *modality* in mind. When considering *transitivity* as conducting the CDA, the US tries to display no fear of interference and to “show off” to other world leaders that they remain a strong military power, especially in the face of the rise of China and the growing threat Russia poses to its might.

This discourse is most likely present to make the US be perceived as seeing cyber warfare lightly and have an identity as staying in the race of possessing the strongest military when it comes to cyber capabilities too while continue to portray “the others”, mainly Russia and China, as the true villains, as stated by Öberg & Sollenberg (2011, p. 60) which is often seen in news during conflict. This result also aligns with constructivism, as new ideas about cyber warfare entered the collective understanding of the American people and re-created their belief about how to think of oneself (Agius, 2019, p. 88).

6.2.2 Retaliation

2010

Although reporting about cyber *warfare*, little is mentioned about retaliation. In 2010, article E mentions retaliating in the manner of “eye for an eye”: “We should think of cyberattacks as guided missiles and respond similarly, intercept them and retaliate” (Zuckerman, 2010). This type of discourse is important to analyse in regard to morals as retaliation is portrayed as the political legitimacy of the state if a cyber-attack occurs. It underlines the seriousness of cyberwarfare, that this is now war and that “we will not tolerate anyone attacking us”. This was, however, only a plan and a threat of it but not a discourse about an actual retaliation taking place.

2020

In 2020, article G´s heading states to combat cyberwarfare “with paper”. This type of discourse comforts the reader and conveys the morals that the US will not pursue military action when combating cyberwarfare but will instead use soft power. Further, only article H mentions a retaliation by a cyber-attack – Trump admitted the cyber-attack on Russia as retaliation for their interference in the 2018 mid-term election. The results demonstrate, in line with constructivism, the changed ideas and morals regarding the appropriateness of what type and how much use of force is legitimate to retaliate with (Agius, 2019, p. 77).

6.3 What is not said?

There are similarities in the discourse in both years regarding what is *not* said. Apart from one article from 2010 and two from 2020, there is little information about the exact plan of how to retaliate. However, the problem remains: who is the actor that should be retaliated against? No article provides a definite answer of who to counterattack – there are only speculations. This links back to the previous research surrounding cyber security: it is hard to identify aggressors wanting to remain hidden in the cyber sphere and even a state, like in the case of Stuxnet, can deny involvement (Dunn-Cavelty, 2019, p. 418).

No article mentions armed attacks, which is part of traditional warfare, or condemn cyber warfare explicitly. Further, no articles mention civilian casualties, despite one comparing it with nuclear weapons, which causes significant casualties when used. Only article K touches on casualties by mentioning that cyber warfare in the future could be considered more morally justifiable because of no causalities. The results are again supported by constructivism, there are – to the authors knowledge – no civilian casualties caused by cyber warfare yet. Therefore, the idea and understanding about it has not yet been established, and hence there is no discourse linked to it since the meaning of it is not currently understood or constructed (Agius, 2019, p. 89)

7 Conclusions

The aim of this thesis was to provide an interpretivist-constructivist insight into cyber security by critically analysing the US media discourse on “cyber warfare” and the use of cyber weapons in the US. The exact research question was: *Given the discourse in US news media since Stuxnet, how have the informal norms regarding “cyber warfare” changed in the last ten years in the US?* The years 2010 and 2020 were examined using a critical discourse analysis of open-source news media – 12 newspaper articles were selected from the New York Times, the Washington Post and the Wall Street Journal – to study the ideas and morals surrounding cyber warfare and any changes that had occurred.

The thesis highlights the degree of ambiguity observable in the terminology of cyber security in academic literature and news media. The aim of the analysis was to investigate the term cyber warfare, which is a debated term. The empirical results provide insight into how Stuxnet influenced and was influenced by the American people, their ideas and morals regarding cyber warfare, and again in 2020 during the US election. The analysis demonstrates that the discourse surrounding cyber warfare in the US news media has changed over the last decade. Drawing on this, the results of the critical discourse analysis prove that the informal norms, ideas and morals regarding cyber operations between 2010 and 2020 have changed *significantly*.

The central changing and emerging ideas about cyber warfare in the US between 2010 and 2020 were: (1) what cyber warfare is – the idea that cyber warfare is new and fearsome has declined. Today, it is merely one of many issues on the political agenda and overstating the danger it poses is more detrimental than it is beneficial; (2) What cyber weapons are – while originally associated with Stuxnet, the idea today seems diffuse and indeterminate; (3) Objective – in 2010, the idea is that cyber warfare targets critical infrastructure, whereas in 2020, the objective of cyber warfare appears to apply to any cyber acts, including incidents that appear more appropriately defined as espionage.

Further, (4) future – the belief the world would encounter a dark and uncertain future resulting from this new type of warfare became, by 2020, there being no unified idea and, in some cases, contradicting ideas. For example, there will be more awareness in the future as we become more reliant on digitalisation, so cyber space will be a double-edged sword that presents opportunity *and* risk in 2030 – cyber warfare might result in cyber *peace* or instead develop a new type of war involving AI, which make the world more vulnerable than it is today.

The central changing and emerging morals were: (1) the self and others – the US discourse promoting “the self” as victims in cyberwar and expressing the underlying idea “this is not who we are” changed to openly admitting conducting cyberwarfare; (2) retaliation – the idea of retaliating is only as present as the *threat* of it. Only one article in 2010 mentioned retaliating by the same means, whereas one article in 2020 mentions retaliation but as a soft approach. Last, central ideas and morals not mentioned include: (1) civilian casualties – not mentioned in any year despite discussions concerning cyber *warfare*; (2) retaliation – more specifically, against who? Since no one claims responsibility or condemns cyberwar, an actual actor is never mentioned – only actors who are suspected (Russia and China mentioned both years, additionally Israel in 2010 and Iran 2020)

These findings identify first, the ambiguity in the terminology for cyber security and the implications this has on comprehension in this area. Second, the importance of analysing news media discourse and the role mass media plays in relation to social change and vice versa. Third, the importance of understanding the unique attributes of the US society in relation to cyber security and the everyday Americans understanding of cyber warfare. It further proves *all* five key principles of constructivism such as that people base their understanding on previous experience, and that informal norms emerge and change over time. Therefore, this thesis contributes to the existing (neo)positivist and technical research in cyber security by complementing with a normative analysis.

The results obtained indicate that the aim of this thesis was achieved. That is, to provide the field of cyber security with an alternative lens where socially constructed knowledge such as ideational and moral factors can explain emerging informal norms regarding cyber warfare in the US and contribute towards a more holistic understanding. We must continue the pursuit of understanding cyber security, the need to develop our capabilities and skilled professionals to deal with it, both now and in the future.

8 Discussion

This thesis produces important findings about informal norms in the US regarding cyber operations, cyber weapons, and cyber security and how they have changed in the last decade. Five findings are particularly interesting and open for discussion.

First, the analytical results strongly align with previous research surrounding the debatable and current non-universal terminology (see for example Andress, & Winterfeld, 2014; Dunn-Cavelty, 2019; Rid, 2013). Despite the rapid digital developments, the implemented policies for conduct in the cyber sphere and the constant media attention about cyber security, cyber operations are still not generally understood (Angstrom & Widén, 2015, p. 107),

In only ten-years, the terminology in cyber security has become more confusing and substantially more misused. The discourse from 2010 has changed from being coherent in the reporting and presentation of similar ideas and morals concerning cyber operations, to being rather incoherent in 2020. The underlying ideas and norms about what cyber warfare is has changed considerably to a broader idea that seems to now include most cyber activities. For example, even low-level incidents in the cyber sphere or cases of cyber espionage are referred to as cyber warfare (Lindsay, 2013, p. 374). This means the ideas about cyber warfare in 2010 can be linked back to discourse 3 – national security– while the ideas in 2020 lean more towards discourse 2 – cyber-espionage (Dunn-Cavelty, 2019, pp. 415-420).

Further, cyber security in 2020 is seen as an integral part of international law but is now more perplexing than before. One only needs to consider the critique of the coherency and terminology in the Tallinn Manual 1.0 (Schmitt, 2013) and Tallinn Manual 2.0 (Schmitt & Vihul, 2017) as seen in *section 1.2*. The meaning of cyber warfare in the Manuals is currently debated and a parallel can be drawn with the discourse in the media since the discourse now has no focus. It also demonstrates that the US must understand its own norms as well as the international norms regarding cyber warfare to achieve stability and agreement on them. It provides an important message for policy makers to act and strive to develop coherent terminology, work towards coherent cyber deterrence and to clearly define areas of responsibility. One way this could be achieved is to create a Tallinn manual 3.0, where clear definitions are given.

Second, the findings strongly align with the theoretical framework constructivism. For example, individuals in society base their understanding and meaning on previous experiences and new ideas emerge (Agius, 2019, pp. 79-78). This is demonstrated by the idea about cyber warfare and weapons was only vaguely established in 2010 and the analysis demonstrates a clear pattern in ideas how Stuxnet shocked the US and was anticipated to be the next big thing in warfare – as demonstrated by Stuxnet being compared to nuclear weapons (see *article F*). The ideas about cyber warfare were somewhat placated by 2020 and became part of everyday discourse. This is clearly demonstrated in 2020 by the fact that cyber weapons analogous to Stuxnet are no longer mentioned. Instead, the ideas about cyber warfare are associated with espionage and article K even speculates about the possibility of a future "cyber peace" (see *section 6.1.4*).

Third, in relation to morals, it is interesting to elaborate upon the discourse about "this is not who we are" in 2010 (see *section 6.2.1*), and that this discourse might re-emerge in the future if AI is used in a similar fashion as Stuxnet. That is, will states resume denying any responsibility in future conflicts involving the cyber sphere? What is not explicitly said might be that the advancement in technology and the constant developments in AI could suggest that the US will try and test the limits of the cybersphere to identify what is acceptable by international standards. Futher, to perhaps see the reactions of whether it is morally acceptable or not, which may have been the case with Stuxnet since not one article in 2020 condemns the attack.

Fourth, it is interesting to discuss the few informal norms that have remained *the same*. For example, that the main aggressors in cyberwarfare are speculated to be Russia and China. This aligns with constructivism since ideas and morals shape identity, and the US appears to want to emit a strong persona to its longstanding adversaries (Aguis, 2019, p. 78). It also aligns with CDA while keeping transitivity in mind – it can be associated with the geopolitical dimension and the pursuit of the US as having *powe*r and *authority* in international relations and in line with constructivism, wanting to portray themselves as "the good ones" compared to the "bad ones" (Boréus & Bergström, 2017, p. 156). This thesis therefore demonstrates the importance for decision makers to be receptive to changes in informal norms when navigating international relations with allies and adversaries alike with regards to cyber security. Ideational research is needed to constantly be one step ahead in the development of *cyber deterrence*.

Fifth, the results also align with the method CDA. There is a clear pattern in the discourse and thus, the informal norms, after analysing only 12 articles. One concern the author had was that no pattern would be observable from so few samples. Further, CDA says discourse changes throughout history, and stresses the importance of media and its power in society – media not only reflect the ideas of society but influences the perception of the public as well (Dunn & Neumannm 2016, p. 36). This highlights the issue caused by the ambiguity in the terminology in cyber security *once again*. The flaws in the medias reporting must be acknowledged to ensure the debates concerning cyber security can improve and society should aim to stimulate a *healthy* debate about issues concerning cyber operations.

In summary, the pursuit of understanding the public perception about the changing informal norms surrounding cyber operations is vital (Dunn-Cavelty, 2019, p. 411). This thesis emphasises the importance of using the interpretivist paradigm in war studies and how important it is to complement the traditional neo-positivist thinking using a normative approach to understand the underlying social phenomena it overlooks. Future research is therefore essential in further understanding what cyber security is, how cyber operations are viewed and how quickly informal norms change.

9 Future research

Although the interpretivist approach to research focuses on contextuality and acknowledges that each case is unique (Schwartz-Shea & Yanow, 2012, p. 113), this thesis demonstrates issues worth researching in future. Three future research suggestions about cyber operations are recommended in line with interpretivist research.

First, research should include a in-depth CDA that is preferably applied to a larger volume of data that utilises both “high data”, which includes books, doctrines, and press conferences, and “low data” such as news articles, blog posts and documentaries viewable on YouTube and its comment sections etc (Weldes, 2014, pp. 228-237). This may uncover a more comprehensive answer and generate a greater understanding of the underlying informal norms regarding “cyber warfare”, and how language is used to influence the society and vice versa.

Second, another pressing issue is owing to the ambiguous terminology which stems from the lack of universal definitions and coherent understanding of terms in cyber security. Historical research on linguistics of specific definitions can help provide clarity to the cyber security debate. Using *histories* as both a method and theory may help advance research in the discussions on the concepts concerning cyber security.

Last, future research should examine the changes in informal norms regarding soldier ideals from a critical feminist perspective. Traditionally, a soldier is associated with masculine traits (Kennedy & Dingli, 2019, p. 160). Yet how is the ideal soldier viewed today when considering the incorporation of the cyber sphere into the battlefield? Future research in these areas are required urgently yet should remain a long-term project since new data continuously emerges.

References

Agius, C. (2019). Social Constructivism. In *Contemporary Security Studies* (5th Ed.). Oxford University Press

Andress, J., & Winterfeld. (2014). Cyber Warfare: techniques, tactics and tools for security practioners (2nd Ed.). Syngress

Angstrom, J., & Widén, J. (2015). Contemporary military theory: the dynamics of war. Routledge

Banasik, M. (2016). Unconventional War and Warfare in the Gray Zone. The New Spectrum of Modern Conflicts. *Journal of Defense Resources Management*, *7*(1(12)), 37–46.

Boréus, K., & Bergström, G. (2017). Analyzing text and discourse: eight approaches for social sciences. SAGE

Bracken, K., & Eaton, A. (2020, October 18). How Will the U.S. Combat Election Day Cyberwarfare? With Paper. *NYTimes.com Feed*. https://www.nytimes.com/

Broeders, D., & van den Berg, B. (2020). Governing Cyberspace: Behavior, Power and Diplomacy. In *Governing Cyberspace*. Rowman & Littlefield Publishers.

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber)security actor? *Journal of Common Market Studies*, *55*(6), 1254–1272. https://doi.org/10.1111/jcms.12575

Chon, G. (2016, July 29). *Review: Iran cyber hack opened a Pandora´s box*. [Editorial]. https://www.reuters.com/article/idUS110404463620160729

Cision Media Research. (2019, January 04). Top 10 U.S daily newspapers [blog]. https://www.cision.com/2019/01/top-ten-us-daily-newspapers/

Clarke, R.A. (2020, October 09). Will we have a Cyberwar or Cyber peace? Richard A. Clarke, a former White House counterterrorism and cybersecurity chief, offers two competing visions of 2030. *The Wall Street Journal*. https://www.wsj.com/

Clausewitz, C. von. (1832). *Vom Kriege*. Ullstein

Collins, A. (Contemporary Security Studies (5th Ed.). Oxford University Press

De Young, K. (2020, October 22). Biden´s foreign policy theme: ‘America´s back’. *The Washington Post*. https://www.washingtonpost.com/

Dulić, T. (2011). Peace Research and Source Criticism. In *Understanding Peace Research: Methods and Challenges.* Taylor and Francis

Dunn, K., & Neumann, I. (2016). *Undertaking discourse analysis for social research.* University of Michigan Press.

Dunn-Cavelty, M. (2019). Cyber-Security. In *Contemporary Security Studies* (5th Ed.). Oxford University Press

Fairclough, N. (2010). Critical discourse analysis: the critical study of language (2nd Ed.). Routledge.

Fairclough, N. (1992). *Discourse and social change*. Cambridge: Polity Press

Farwell, R., & Rhozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival (London)*, *53*(1), 23–40. https://doi.org/10.1080/00396338.2011.555586

Félegyházi, P. (2012). The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet*, *4*(4), 971–1003. https://doi.org/10.3390/fi4040971

Fitton, O. (2016). Cyber Operations and Gray Zones: Challenges for NATO. *The Quarterly Journal (English Ed.)*, *15*(2), 109-119. https://doi.org/10.11610/Connections.15.2.08

Gorman, S., & Fidler, S. (2010, September 25). U.S. News: Cyber Attacks Test Pentagon, Allies and Foes. *The Wall Street Journal Online*. https://www.wsj.com/

Gragido, W., & Pirc, J. (2011). Cybercrime and espionage: an analysis of subversive multivector threats. Syngress

Greenberg, A. (2019a). Sandworm: A New Era of Cyberwar and the Hunt fot the Kremlin´s Most Dangerous Hackers (1st Ed.). Doubleday

Greenberg, A. (2019b, August 23). The WIRED Guide to Cyberwar. *The Wired*. https://www.wired.com/story/cyberwar-guide/

Guay, J., & Rudnick, L. (2017). *What the Digital Geneva Convention means for the future of humanitarian action*. https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/

Hurd, I. (2008). *Constructivism*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199219322.003.0017

Joint Chiefs of Staff. (2018, June 08). Cyberspace operations, Joint Publication 3-12 [unclassified version]. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150

Kennedy, C., & Dingli, S. (2019). Gender and Security. In *Contemporary Security Studies* (5th Ed.). Oxford Univeristy Press

Libicki, M. (2012). "Cyberspace is not a warfighting domain" *I/S: A journal of law and policy for the informaion society, 8*(2): 325-40.

Lindsay, J. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Maclean, W. (2010, December 19). A destructive Internet worm could be potent cyber weapon. *The Washington Post*. https://www.washingtonpost.com/

Madrigal. A. (2011, March 04). 'Stuxnet is the Hiroshima of Cyber War'. *The Atlantic*. https://www.theatlantic.com/technology/archive/2011/03/stuxnet-is-the-hiroshima-of-cyber-war/72033/

Markoff, J. (2010, October 03). A Code for Chaos. *The New York Times*. https://www.nytimes.com/

Markoff, J., & Sanger, D.E., & Broad, W.J. (2010, September 30). In a Computer Worm, a Possible Biblical Clue. *The New York Times*. https://www.nytimes.com/

Mazanec, B. (2015). The Evolution of Cyber War: International Norms for Emerging-Technology Weapons. Potomac Books

Mello, J.P. (2020, October 01). *Cyberwarfare report, Vol 5, No. 3: U.S Election security threats and warnings.* Retrieved from https://cybersecurityventures.com/cyberwarfare-report-q4-2020-u-s-election-security-threats-and-warnings/

Möller, F. (2011). News Reports versus Written Narratives: Collecting Information using different types of empirical sources in *Understanding Peace Research: Methods and Challenges.* Taylor and Francis

Nakashima, E. (2010, October 02). Stuxnet malware is blueprint for computer attacks on U.S. [Corrected 8 Oct 2010]. *The Washington Post*. https://www.washingtonpost.com/

Nakashima, E. (2020, October 30). Overstating foreign threat to election poses its own risks, U.S officials and experts say. *The Washington Post*. https://www.washingtonpost.com/

Nicander, L., & Ranstorp, M. (2004). *Terrorism in the information age: new frontiers?* Försvarshögskolan

Nyberg, R., & Tidström, A. (2012). *Skriv vetenskapliga uppsatser, examensarbeten och avhandlingar* (2., [rev.] uppl. / redaktörer: Rainer Nyberg, Annika Tidström). Studentlitteratur.

Oltsik, J. (2020). *The Life and Times of Cybersecurity Professionals 2020*. The Enterprise Strategy Group. https://2ll3s9303aos3ya6kr1rrsd7-wpengine.netdna-ssl.com/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf

Omand, P., & Pythian, M. (2018). *Principled Spying: The Ethics of secret intelligence*. Oxford University Press

Ranger, S. (2018, December 04). *What is cyberwar? Everything you need to know about the frightening future of digital conflict*. Retrieved from https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

Rid, T. (2013). *Cyberwar will not take place*. Oxford: Oxford University Press

Ringmar, E. (1996). Identity, interest, and action : a cultural explanation of Sweden's intervention in the Thirty Years War. Cambridge University Press.

Risjord, M. W. (2014). *Philosophy of social science : a contemporary introduction* . Routledge, Taylor & Francis Group.

Russell, A. (2014). *Cyber blockades*. Georgetown University Press

Sanger, D.E. (2020, July 11). Trump Claims Credit for 2018 Cyberattack on Russia. *NYTimes.com Feed*. https://www.nytimes.com/

Schmitt, M. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press by NCCDCE

Schmitt, M., & Vihul, L. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press by NCCDCE

Schwartz-Shea, P., & Yanow, D. (2012). *Interpretive research design concepts and processes.* New York, NY: Routledge.

Stone, J. (2013). Cyber War will take place. *Journal of strategic studies, 36*(1), 101-108.https://doi.org/10.1080/01402390.2012.730485

Talley, I. (2020, October 08). U.S. Sanctions Additional Iranian Banks; Move aims to sever few financial connections Teheran still has to world. *The Wall Street Journal*. https://www.wsj.com/

Tannenwald, N. (1999). The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use. *International Organization, 53*(3), 433–468. https://doi.org/10.1162/002081899550959

Thurén, T. (2019). *Källkritik* (J. Werner (Ed.); 4th Ed.). Liber.

Treverton, G. (1988). Covert action: the CIA and the limits of American intervention in the postwar world. Tauris.

Uren, T., Hogeveen, B., & Hanson, F. (2018). *Defining offensive cyber capabilities*. https://www.aspi.org.au/report/defining-offensive-cyber-capabilities

Walzer, M. (2016). *Just and unjust wars: a moral argument with historical illustrations* (5th Ed.). Basic Books, a member of the Perseus Books Group

Weldes, J. (2014). *High Politics and Low Data. Globalisation Discourses in Popular Culture*" in Yanow, D., & Schwartz-Shea, P., (eds). Interpretation and Method Empirical Research Methods and the Interpretive Turn. Armonk, NY: M.E. Sharpe.

Wendt, A. (1992). Anarchy is what states make of it: The social construction of power politics. *International Organization*, *46*(2), 391. https://doi.org/10.1017/S0020818300027764

Wendt, A. (1999). *Social theory of international politics*. Social Theory of International Politics.

Zuckerman, M. (2010, December 06). How to fight and win the Cyberwar. *The Wall Street Journal Online*. https://www.wsj.com/

Öberg, M., & Sollenberg, M. (2011) Gathering Conflict Information Using News Resources. In *Understanding Peace Research: Methods and Challenges.* Taylor and Francis