Cyber Dominance as a National Security Strategy:

Sweden's Approach and Global Implications

Damilare Latinwo

Autumn 2024

One-Year Master thesis: 15credits

Supervisor: Ane Kirkegaard

To My Parents for Investing in my Education

Latinwo Ademola and Latinwo Abosede

Abstract

This thesis examines the role of cyber dominance in national security, how the development of cyber capabilities has become a centre of focus in the international system, and how it is important for the power struggles within the global political environment. The study draws focus to Sweden's strategies for developing its cyber capabilities within this context, and the global implications of its actions. The purpose is to understand how cyber power has come to be important for national security strategies, how it is integrated into these strategies, and its impact on global politics.

The research uses a theoretical perspective that considers the historical assumptions of power, particularly the realist perspective, and how they are challenged by cyber developments. Sweden's security policies over the years is interrogated, shedding light on the updates and reforms the country has incorporated to address growing cyber threats. Key findings reveal that Sweden has chosen to focus on developing cyber resilience, collaborating with other actors in the international system towards balancing its defensive and offensive cyber capabilities.

Keywords: *Cyber Dominance, National Security, Sweden, Cyber Strategy, Power*

Word Count: 12,061 (minus Abstract, Table of contents and References).

Table of Contents

Chapter One: Introduction

"Information is the oxygen of the modern age… It seeps through the walls topped with barbed wire. It wafts across the electrified, booby-trapped borders. Breezes of electronic beams blow through the Iron Curtain as if it was lace."

— Ronald Reagan (L.A Times, 1989)

Realism as a major theory in international relations and global politics places great emphasis on the importance of power, security and dominance in the international system. Realists contends that the primary concern of a state is to ensure its survival and security in an anarchic global system where no central authority exists. They advance that states must do all within their ability to secure their national interests, holding strongly to the belief that 'power is the currency of international politics,' and that because of this, states must continuously act to increase their power relative to others (Schouten, 2012; Ylönen, 2022). Historically, power was measured in terms of military strength and economic resources. However, in today's world, this power has evolved to not just encompass military capabilities and economic prowess alone, but the advent of the digital age has introduced a new dimension of power: 'technological power,' of which cyber capabilities is one of its forms (Schroefl, 2020; IISS, 2021).

In this current epoch, nations of the world have come to increasingly rely on technology for critical infrastructure, economic stability, and defence (Kala, 2023; Edler et al. 2023). Additionally, the world has become increasingly intertwined due to globalisation and the proliferation of digitalisation, so much that states can now influence each other, impacting directly on economic, social, and even political spheres of counterpart states through the use of digital media, and information has become a new resource to this end (Chin 2019; Burlacu et al., 2021). Asides being a means of influence, technological advancements while bringing so much benefits, have such loopholes that critical and military infrastructures of states can be attacked to either destroy them or to compromise them to attack the given state itself, through hidden cyber-attacks from enemy forces (Geers, 2009; Futter, 2016). The cyberspace has therefore become a critical domain for national security, and the ability to dominate and wield strong influence in this domain is seen as an essential area determining a state's power. Nations of the world now seek cyber dominance mainly to protect their digital infrastructure, deter cyber-attacks, and project power in cyberspace (IISS, 2021). Therefore, achieving cyber dominance in this age is crucial for a state's survival and influence in the international system.

Within this conversation, Sweden, a country which has over the years of its existence been known for its neutrality and commitment to diplomacy, has also recognised the necessity of technological advancement and cyber dominance in safeguarding its national security (Brommesson, Ekengren, and Michalski 2022; ITA, 2023). As cyber threats from state and non-state actors become more sophisticated and pervasive, the ability to defend digital infrastructure and maintain cyber resilience has become a matter of national security for the continued smooth-running of states. This realisation has driven Sweden to strive towards developing a comprehensive approach to cyber dominance to guide and secure its cyberspace while also maintaining relevance within the new digital power order (MSB, 2022).

1.1. Research Problem

From the age of the information war and espionage of the West against the Eastern Bloc during the cold war, up to the moment of the Stuxnet Worm attack by the U.S against the Iranian nuclear development, and several other similar attacks and disinformation spread by Russia and China to influence the international system and allegedly the U.S 2016 elections, amongst cyber-attacks in recent years, (Richardson, 2011; Jensen, 2017; Doshi and Williams, 2018; Bandurski, 2022), cyber warfare has come to the fore of warfare and power play in the international system and global politics. As cyber threats become more sophisticated and frequent, affecting everything from critical infrastructure to government and private sector operations, understanding how nations conceptualise and implement cyber dominance had become important for national and international security.

Additionally, it is necessary to understand that cyber warfare can be inherently asymmetric, meaning that smaller and less powerful actors can potentially cause great amounts of damage on more powerful states. Hence, this asymmetry which is a core characteristic of cyber dominance, presents a problem in the international system (Warchał and Piotrkowski, 2023). Traditional theories of warfare and conversations about the projection of power are mostly based on the assumption of symmetric capabilities, where states with greater resources and capabilities are more likely to prevail. However, in cyberspace, the playing field is more level, and even small actors, for example, non-state actors like terrorist groups, can pose serious threats (Tran, 2018; ORF, 2023).

Meanwhile, there is also the need to take into consideration legality and ethicality of cyber-attacks and efforts to protect national security either in defensive capacity to protect against cyber-attacks, or in offensive capacity to pre-empt either military attacks as in the case of US and the Stuxnet worm attack or other cyberattacks (Yannakogeorgos, 2016; Hayward, 2017;

Moynihan, 2019). Consequently, this research problem is rooted within the realist perspective of international relations which places great emphasis on the importance of power, security and national interests in an anarchic international system, and Sweden's position within the new power dynamics the cyber space brings.

1.2. Research Aims and Objectives

The central aim of this research is to examine how cyber dominance has become a new form of power struggle in the international system, shedding light on its importance for national security, how it is different from traditional-military warfare, its relevance in global politics, and the place of Sweden in this development. The study will first, concentrate on examining the concept of cyber dominance in a bid to evaluate and expound on its importance and differences from traditional conflicts. The research will then interrogate the impact of cyber dominance on global power dynamics and international relations. Sweden's strategies on Cyber dominance will be explored, detailing how the country has developed and implemented cyber policies to ensure security and resilience. Finally, the concept of ethical and legal considerations of cyber operations will be evaluated within the international framework and how Sweden has positioned to navigate these considerations.

1.3. Research Questions

With the research problem and thesis objective in mind, the following research questions will guide this research:

1. How has cyber dominance emerged as a new form of power in the international system?

2. Why is cyber dominance important for national security?

3. What is Sweden's approach to cyber dominance, and the global implications the country's approach?

1.4. Relevance to Global Politics

The concept of cyber dominance has come to become an increasingly relevant and controversial topic in global politics. Before now, the focus of power in international relations has always been on military, economic, and diplomatic strength. However, the emergence of cyberspace as a new arena of competition has greatly changed how power is understood and exercised. The peculiarities of cyber capabilities are now that it allows states to achieve political, economic, and military goals without having to engage in physical conflict (Cavelty and Wenger, 2022; Martino, 2023). Hence, this evolution affects the theories of power,

sovereignty, and security in international relations. Scholars like Robert Keohane, Joseph Nye, and James Lewis amongst others have interrogated the concept of cyber power, bringing to light its importance for national security and global politics, as it enables states to exert influence and achieve its strategic objectives in cyberspace (Keohane and Nye, 1998; Nye, 2011; Carr and Nye, 2018; Lewis, 2020)

Cyber dominance also relates to broader socio-political issues as it concerns the well-being and integrity of states. For example, cyber-attacks on essential infrastructure, such as power grids, financial systems, and communication networks, can severely affect the national security and economic stability of countries (Li and Liu, 2021; Kala, 2023;). Additionally, the protection of personal data and privacy is very important, as cyber espionage and surveillance pose ethical and legal challenges due to its negative impacts on citizens and as a result, the state ((Tronnier *et al.*, 2022, pp.238.; Olaoye, 2023; Natalucci, Qureshi, and Suntheim, 2024). By analysing Sweden's approach to these issues, this research seeks to enhance the understanding of how this power structure has developed, and how countries can create effective cybersecurity strategies that balance security, privacy, and ethical considerations while still achieving its strategic objectives in the international system.

1.5. Thesis Structure

This thesis is structured into five main chapters. **Chapter 1**, which is the 'Introduction,' lays the foundation for the research topic, explaining why it is important within the field of global politics. Here, the main problems the research seeks to interrogate and the research questions are outlined, as well as the aims and objectives of the research. This is followed by a literature review and theoretical framework in **Chapter 2.** This chapter explores existing research on cyber dominance, national security, and Sweden's cybersecurity policies, analysing what other researchers have found and discussing their ideas.

Chapter 3, is the 'Methodology,' which describes how the study was conducted. This section explains how data was collected and analysed, why these methods were chosen, and reflects considerations about the ethical aspects of the research. **Chapter 4**, the 'Analysis,' presents the study's findings, discussing what was discovered about cyber dominance, its importance for national security, and how Sweden approaches this issue. These findings are linked back to the research questions and theories discussed in Chapter 2. Finally, **Chapter 5,** the 'Conclusion,' summarises the main findings and discusses what they mean for global politics and national

security. It reflects on the methods and theories used, acknowledges any limitations, and suggests areas for future research.

Chapter Two: Literature Review/Theory

This chapter explores existing literature on Cyber power and cyber dominance and its interrelations with national security in the international system. It expounds on what has been written by scholars, experts and governments touching on key themes and discussions around cyber dominance, its impact on national security, its unique characteristics compared to traditional warfare and as a new form of power struggle within global politics dynamics, and a short overview of where Sweden stands within this conversation. The chapter is organised into three main sections: 'The Concept of Cyber Power and Cyber Dominance,' 'National Security in the Digital Age,' and 'Overview of Sweden's National Security Strategies Within the International System.' This chapter then concludes with an exposition of the realist theory as the theoretical underpinning for the research and why it bears great relevance to this study.

2.1. The Concept of Cyber Power and Cyber Dominance

While conversations about cyberspace, its peculiarities and importance to national security is seemingly a new—21st century conversation as relating to power and conflict dynamics in the international system, 'information' have always been a core defining element in wars, power struggles and state pursuit of dominance. This is because adequate information about the forces, disposition, and weaknesses of a state are important in the ability to overwhelm the states and exploit their weaknesses to win against enemy nations (Pressel, 2021; McNeilly, 2015). According to Singer (2001) Sun Tzu's teachings on information warfare provides a great exposition into how information systems are used as early as back in the earlier centuries to disrupt or manipulate an opponent's knowledge and communications with the aim of gaining advantages at a low cost, and can either supplement or replace traditional military methods. However, increased digitalisation and technological advancement in recent epochs which seeks to make life much easier, automated, and increase efficiency have made it such that large amounts of information are kept in databases and floating on the web—even if in seemingly secured spaces—and systems are interconnected across the world one way or the other, leading to the evolution of a new space: the cyberspace (Malik and Choudhury, 2019; Reveron and Savage, 2023).

The cyberspace has been conceived to be different things by scholars, drawing first from William Gibson, who coined the word, saying that "Cyberspace is a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts … A graphic representation of data abstracted from the banks of every computer in the human system" (Malik and Choudhury, 2019). Bryant (2001) posits that

Cyberspace embodies a virtual place of communication and connectivity, in which four main sub-concepts of ‘place,’ ‘distance,’ ‘size’ and ‘route’ meets and bears great relevance as in physical spaces, but more in the sense of hardware and software and human interaction within this environment. Similarly, Ottiss and Lorents (2010) advance that “cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems.” A study by Štrucl, (2021) highlights several layers of cyber space as it has influence and is interconnected from the physical layer including infrastructures and hardware, the network and information layer, down to the social layer which encompasses its influence on human social interaction including media, emails, telephones and more. Hence, it is within this whole context that Cyber power has come to the limelight.

According to van Haaster (2016), cyber power involves the ability to exert influence within or through cyberspace, which includes various forms of power that affect how individuals and entities interact in this digital domain. Kuehl (2009) in establishing a definition of Cyber power takes a cue from other domains wherein military and economic power is reflected, including air, land and sea, thereby propounding that cyber power is the ability to make use of cyberspace effectively, shaped by technology and the goals of organisations. He goes further to explain that cyber power enhances political, informational, military, and economic activities, transforming how data is created and used, and connecting people and organisations in new ways across traditional boundaries. Similarly, Nye (2010) posits that power varies by situation, and cyber power is based on the resources available in cyberspace. He argues that cyber power depends on resources like 'infrastructure,' 'networks,' 'software,' and 'human skills' for managing electronic information, advancing that this power allows for achieving desired outcomes in cyberspace and even to other areas outside this space, using interconnected digital resources.

Bringing the definition down into politics and international relations, Nye (2010) asserts that cyber power has become a very important aspect of global politics which is redefining traditional notions of power and influence. This concept encompasses the ability of a state or organisation to make use of cyberspace to achieve strategic objectives, assert dominance, and influence other actors in the international system. This definition therefore embodies the manifestations of cyber power which could be in various forms from cyber warfare, cyber espionage, cyber diplomacy, to the control of information flows (Biller and Schmitt, 2019; Cavelty and Wenger, 2022). Kramer, et al. (2007) in critically engaging the various environmental theories of power develops a holistic framework for the development of a theory

of definition of Cyber power as it influences the socio-political and international environment as highlighted below.

Common Features of Environmental Power Theories	Implications for a Theory of Cyberpower	Observations
Political-Military impact of technological trends	New realm for political dialogue and conflict	Blogging Terrorist use
Pace and scope of operations	Ever increasing speed	Slammer worm Video of beheadings
National mobilization of key resources	Management of cyberspace as a joint economic/military domain Centrality of human resources	Contrasting approaches (e.g., US, China) Locus of expertise in commercial sector
Recognition of logistics and Lines of Communications (LOCs)	Physical Logical	Long haul, interconnection points Logical standards/mgt of IP
Gaining control of key features	Physical Code/logical assets	Undersea cables, satellites Governance in a global community

Kramer et al (2007) on developing a theory of cyber power

Cyber dominance is, therefore, the extent to which a state or organisation can make use of the cyberspace to enforce its own goals, protect its resources, and prevent its adversaries from doing the same. This concept encompasses not only offensive capabilities but also defensive measures, seeking to make sure that the integrity, availability, and confidentiality of information systems are kept securely (Voo et al., 2020). Stytz and Banks (2014) conceives of cyber dominance more in form of strategic advantage. They advance that it is practically impossible for a single state to achieve global cyberspace dominance or total control of the entire international cyberspace architecture. Hence, states must seek to dominate in specific areas which are critical and strategic to their existence and power posture both as a form of strategic advantage and also a form of deterrence to other states. However, the U.S Department of Navy (2023) asserts that complete cyber dominance which involves overall superiority in cyber intelligence, cyber operations, and cyber defense mechanisms is important due to the ever -evolving nature of the cyberspace, the increasing sophistication of cyber threats, and the critical need to protect national security, economic interests, and sensitive information from adversaries. This, therefore, brings back the arguments of realists on anarchy, power-struggle, national interest, and self-help into the conversation and peculiarities of Cyber dominance.

2.2. National Security in the Digital Age

Over the years of scholarly and philosophical postulations about the state and its need to protect itself against external foes and aggression, the concept of 'National interests' and 'National security has stood out in global politics and international relations as core topic areas. Liu (2014) defines national interests as "encompassing the political interests, security interests, economic interests, cultural interests and other interests of a country," with national security taking precedence in the pursuits of states. Meanwhile, while several scholars, experts and national organisations including Holmes (2015), New Zealand Department of the Prime Minister and Cabinet (2017), and Wyrębek (2022) all at the core of their submissions agree that national security encompass the protection of the citizens, a state's political sovereignty, economy, critical infrastructure, and institutions of a country from both internal and external threats, to ensure the safety, stability and wellbeing of the nation. However, Williams, Cimbala, and Sarkesian (2022) advance that national security policies filter into foreign policy and international relations as countries strives to protect their interests within this environment and accrue more benefits for themselves. This has cast the term in certain levels of ambiguity, especially as touching the issue of aggression against other states seemingly to pre-empt an attack from them in the name of national security, with an example being the US attack on Iran and its nuclear efforts over the years based on these same grounds (Dunn, 2007; JINSA, 2023). The advent of cyberspace and cyber power has only served to further expand the frontiers of national security and what it constitutes.

In this digital age, national security has been broadened to include the protection of information systems and digital infrastructure, as technological advancements have introduced new weaknesses and threats for countries (Al-Tae, Al-Dhalimi and Shaibani, 2020). Hence, states strive to protect key trade secrets and information that could affect its economic interaction with other countries, military capabilities and remote-control capacity, citizens data, and information about key institutions and decisions amongst others as highlighted by the governments of the U.S, U.K, Sweden, amongst others in their Cybersecurity strategy documents (Cyberwiser, 2021; HM government, 2022; The White House, 2023). This has introduced new peculiarities and challenges for states to tackle within the international system, impacting military, economic and social aspects of countries and also interrelations between them.

Additionally, cyberwarfare has come to the fore of peculiar changes impacting national security and its dynamics. Petru-Cristian (2024) contends that cyber warfare is unlike traditional

conflicts, which involve physical battles with clearly identified combatants, rather taking place in the digital realm with anonymous actors using hidden tactics. Digital attacks in cyber warfare aim to disrupt, damage, or destroy information systems, networks, and critical infrastructures, and it is most times difficult to identify actual attackers and retaliate against them (Iftikhar, 2024). This warfare brings in great elements of asymmetry, allowing smaller states and non-state actors to challenge larger, more powerful adversaries with as much as little cyber capabilities using easily affordable resources (McFarland, 2011). Many cyber-attacks focus on disruption rather than outright destruction, aiming to undermine public confidence, cause economic disruptions, or influence political outcomes without physical confrontation. Meanwhile, non-state actors, including terrorist organisations, criminal groups, and hacktivists, use cyber tools to achieve their goals independently or as proxies for state actors, for example, the hacktivist group Anonymous which has carried out numerous cyber operations against governments and corporations to promote political and social causes. States also sometimes use non-state actors to conduct cyber-attacks, allowing them to maintain the ability to deny responsibility and complicating the process of attributing and responding to these attacks (Canfill, 2022; Handler, 2022; Svyrydenko and Możgin, 2022).

Key changes in national security strategies due to technological advancements include:

1. Integration of Cyber Capabilities

The national security strategies in countries of the world today now include cyber capabilities as a key part of their defence plans. This means developing both offensive and defensive cyber operations to protect their national interests and act as a form of deterrence against enemies. For instance, the United States established U.S. Cyber Command (CYBERCOM) in 2010 to oversee and coordinate its cyber defence and attack strategies, while the country's Department of Navy also rolled out a '2020 DON Information Superiority Vision (ISV) and the 2022 DON Cyberspace Superiority Vision (CSV)' to aid its naval operations within the cyber space and the activities of the CYBERCOM (U.S. Department of Navy, 2023; Lonergan and Montgomery, 2024). Similarly, in the ongoing the conflict with Ukraine, Russia has again and again made use of cyber units to disrupt Ukrainian communications and infrastructure (Diguin and Pavlova, 2023). These examples are merely simpler examples of how nations are integrating cyber capabilities into their military and intelligence agencies to defend against and conduct cyber operations against adversaries in recent times all in the name of national security.

Also, governments have incorporated Cyber intelligence as a critical part of national security. Governments have developed agencies towards gathering intelligence on potential cyber

threats, monitoring threatening activities in cyberspace, and identifying weaknesses within their own systems. Overall, this proactive approach strives to help in pre-empting attacks and formulating effective responses in case such arises (Gilad, Pecht and Tishler, 2020; Ainslie et al., 2023)

2. Protection of Critical Infrastructure

Increased advancements in technology and the digital space have made it such that critical infrastructure, such as power grids, financial systems, and communication networks are increasingly making use of digital technologies to run core aspects of their activities. Hence, national security strategies now emphasise protecting these critical infrastructures from cyber-attacks, as disruptions can have severe results on the economy and socio-political environment. From May 7 to 12, the Colonial Pipeline, which provides nearly half of the fuel for the East Coast of the United States including 'gasoline,' 'diesel fuel,' 'heating oil,' 'jet fuel' and 'fuel' used by the armed forces of the country, was attacked by a ransomware group called DarkSide. As a result of this cyber-attack, the pipeline had to be temporarily shut down, causing great fuel shortages and leading to panic buying in several states. This incidence caused widespread disruption in several services within the affected states and would have had a protracted impact on the economy, daily life on the citizens and even the military if it was not quickly tackled, which was allegedly done by paying the hackers about $5million as ransom (Kaspersky, 2021; CISA, 2023).

Similarly, Polityuk, Vukmanovic and Jewkes (2017) reports that in 2015, Ukraine's power grid was targeted in a cyber-attack which temporarily disabled power for over 200,000 people for several days. Several other instances of such attacks on different state infrastructures have made governments to devise methods of protecting important infrastructure, including even collaboration with private sector entities to enhance the resilience and security of these infrastructures (Ackerman, 2021; CISA, 2024).

3. Adaptation to Hybrid Warfare

Cristiano and van den Berg (2023) advance that the introduction of Cyberwarfare has led to the incorporation of hybrid warfare. This embodies a situation in which states make use of a mix of traditional military strategies in conjunction with cyber operations and information warfare to meet their goals in conflicts situations and actual warfare. Examples of these form of warfare includes the use of disinformation and fake news which seeks to compromise the internal integrity of state, or misinform military campaigns to make terrible errors. Consequently, national security strategies have been forced to adapt to these complex threats

by developing ways to counter disinformation campaigns, cyber-attacks, and other unconventional forms of aggression.

4. International Cooperation and Norms

The global, far-reaching and continual evolving nature of the cyberspace has made international cooperation come to the fore-front of cybersecurity strategies for like-minded countries. Tewari (2019), EU CyberNet (2023), and Iftikhar (2024) all posit that due to this threat, nations all over the world are compelled to come together to work on various cybersecurity projects, sharing information about threats, and striving hard to create rules for responsible behaviour in cyberspace. This collaboration aims to prevent cyber conflicts and maintain stability in the digital world in a bit, making it safer and more secure for both states and their citizens.

2.3. Overview of Sweden's National Security Strategies Within the International System

Realists, and even other schools of thoughts in global politics and international relations agree that ensuring national security is the primary responsibility of states within the international system. According to Krebs (2018), this responsibility has a great influence on both domestic policies and how countries relate one to another, with each impacting the other. This makes it such that national security is a dominant concern in both areas, and occurrences within the international system could shape the national security strategy of a country and vice versa. Chin, Skinner and Yoo (2023) posits that national security strategies of countries evolve through the years as they encounter different epochs, each bringing with it unique opportunities, challenges, and requiring new responses.

A backtrack into Sweden's historical development reveals its creation within an extremely volatile period of wars transcending different time-periods, greatly impacting the country's national security strategies (Informationsverige, 2023). Asides during the Napoleonic wars where Sweden initially tried to maintain neutrality but was forced to take a side in the war, the country has always strived to maintain a policy of neutrality and impartiality (non-alignment) in the international system amidst inter-states conflicts, wars and as it touches on its national security (Jonasson, 1973; Marzagalli and Müller, 2016). This approach aimed to keep Sweden out of military alliances and conflicts, especially during the tumultuous periods while focusing on developing its internal strength and maintaining its political sovereignty and territorial integrity. During World War I, Sweden maintained its neutral stance, successfully avoiding

being entangled in the conflict despite pressures from either of the warring parties, and this policy of neutrality carried over into World War II (Tepe, 2007).

Sweden's neutral position allowed it to act as a mediator and provide humanitarian aid. However, it also faced criticism for its economic interactions with Nazi Germany, as it continually engages in trade with them including of essential goods like food (Wahlbäck, 1998; Tepe, 2007). In the Cold War era, Sweden adapted its neutrality into a policy of non-alignment in peacetime, just like the one aimed at maintaining neutrality in wartime. This meant Sweden did not join NATO or the Warsaw Pact during this period, choosing instead to focus on a defence strategy capable of deterring both Western and Eastern bloc powers. To support this, Sweden tried to form a Nordic defence pact with four other nations, Finland, Denmark, Iceland and Norway, which did not fall through as Denmark, Iceland and Norway chose to join NATO. Sweden was consequently forced to invest in a robust national defence system, ensuring it could discourage aggression from either side (Bailes, Herolf and Sundelius, 2006; Cronberg, 2008; Makko, 2012).

The core of Sweden's national security strategy according to the Prime Minister's Office in 2021 advances that "Sweden's freedom, peace and security must be safeguarded. No duty of the State is more important. … Sweden aims to be an open and secure society for all" (Government Offices of Sweden, 2021a), reflecting its strong stance for neutrality, impartiality and responsibility mainly to its people. The country's national security strategy has also always emphasised about playing a strong humanitarian and diplomatic role. Sweden has been very active in international organisations like the United Nations, promoting peace, human rights, and development seeking to complement its national security policy by pushing for global stability and reducing the risks of conflict (ECDPM, 2017; Milante et al. 2021). This blend of neutrality, strong defence, and active international diplomacy has been key to Sweden's approach to national security for long decades.

However, in March 7 2024, Sweden officially joined NATO against the backdrop of Russia's invasion of Ukraine (Edwards et al., 2024). This move represented a departure from its strongly held initial views of neutrality and non-alignment, more so as pressures of imminent Russian invasion became pronounced, and the changes within the international system and the rise of Cyber security challenges called for more global cooperation to ford through (Kiderlin, 2024; Reuters 2024). The speech of the Minister for Foreign Affairs Tobias Billström towards their joining of NATO captures the underlying reasons for this move more, as he remarks that:

> *"Sweden is joining NATO at a time when emerging technologies lie at the core of geopolitical competition and play an important role in the defence of Ukraine. We want to contribute to maintaining NATO's technological edge and countering threats in the cyber domain. Swedish strategic assets include an advanced private sector – not least in telecommunications – a strong defence industry and a national space capability in the making" (Government Offices of Sweden, 2024a).*

Meanwhile, as technology advanced and the digital age came into being, Sweden was among the first countries to recognise the opportunities available within this development and to also adopt it in their systems and society (Petterson, 1994; Bäckström, 2001; Pashkevich, Haftor, and Pashkevich, 2021). However, this also enabled them to quickly become aware of the weaknesses available within the digital systems. Hence, Sweden understood that integrating cybersecurity as a component of the country's national security and evolving its approach to address the challenges posed by the cyberspace was necessary. In the late 1990s and early 2000s, Sweden began to make efforts towards establishing a system of protection within the cyberspace with a focus on protecting critical infrastructure and government systems by establishing provisions within the country's legal and regulatory frameworks including: the 'Protective security Act of 1996,' 'Archives Act of 1990,' 'Personal Data Act of 1998' and the 'Electronic Communication Act of 2003' amongst others (Swedish Government, 2017).

Over the years, the Swedish government have created and empowered several institutions and agencies with the duties of enhancing the country's cyber resilience, response to cyber incidents, and promotion of awareness and education for its people about cybersecurity. These agencies include: "the 'Swedish Civil Contingencies Agency (MSB), the National Defence Radio Establishment (FRA), the Swedish Defence Materiel Administration (FMV), the Swedish Armed Forces, the National Post and Telecom Agency (PTS), the Swedish Police Authority and the Swedish Security" (Swedish Civil Contingencies Agency (MSB, 2020a). Additionally, in recognition of how the threat of cyberthreat can spread across international borders, Sweden has actively participated in international cybersecurity efforts, collaborating with the European Union, NATO (as a partner country at the time), and other international organisations to share intelligence, and try to create a semblance of rules and norms to guide operations in the cyberspace (Swedish Government, 2017). Consequently, Cybersecurity has come to feature as a key part of Sweden's national security strategy at present.

2.4. Theoretical Framework

This thesis is rooted in realist assumptions which emphasise the importance of power, security, and survival in an anarchic international system where no central authority exists. According to Realist thought, states must hold their national interests as priority, engaging in self-help and continuously work towards increasing their power relative to others (Usiemure and Gbigbidje, 2018; Antunes and Camisão, 2018). Historically, this power used to be measured primarily in terms of military strength and economic resources. However, the technological and widespread digital landscape of today's world has caused the concept of power to expand to include technological capabilities, particularly in cyberspace (Nye, 2010; Meierding and Sigman, 2021).

The emergence of cyber dominance, which involves the ability to control and make use of cyberspace to achieve national security objectives, fits neatly within the Realist framework.f It represents a modern extension of the traditional quest for power and security, bringing to light how state adapt their strategies to the new realities brought about by technological growth (Nye, 2010; Schroefl, 2020). By focusing on cyber dominance, states like Sweden aim to protect their critical infrastructure, deter cyber-attacks, and maintain their sovereignty in the cyberspace (Swedish Government, 2017). This is in line with the Realist assumption that states must employ all available means to ensure their security and maintain their power, especially through engaging in self-help (Antunes and Camisão, 2018). Therefore, using Realist theory to analyse Sweden's cybersecurity strategy will help to provide an in-depth understanding of how cyber dominance has become an important element of national security in the present world, expounding also on the continued relevance of power dynamics in shaping the behaviour and relations of states in the international system.

Chapter Three: Research Methodology

This chapter outlines the research design and methodology for this thesis. As highlighted in Chapter One, the primary aim of this research is to shed light on how cyber dominance has brought about changes in the power situations of global politics, and to explore Sweden's cyber dominance strategy and its implications for national security and the international system. This chapter explains the methods used including data collection, sources of data, and type of analysis that will be engaged amongst others. The justification for these methods and ethical considerations related to this research are also expounded.

3.1. Research Design

According to Khanday and Khanam (2019), research design is a structured plan for conducting research which brings together methods and techniques to logically and efficiently address the research problem and serve as a guide for the research process. In this thesis, a qualitative research design is engaged. The decision to use qualitative methods aligns with the research goals of this research, which seek to thoroughly understand the concept of cyber dominance as a form of power and national security strategy, its evolution, and Sweden's cyber strategy within this. Creswell and Poth (2018) state that qualitative research is especially useful for studying issues that are seemingly complex and getting a detailed view of particular situations.

3.2. Data Collection

3.2.1 Types of Data

The research relies on multiple sources of qualitative data, including:

1. **Books and Journals**: Academic literature provides great source of information which will aid the analysis of this research. Relevant books and journal articles on cyber dominance, national security strategies, and Sweden’s specific approaches will be reviewed and incorporated into the research to rigorously interrogate the research questions (Snyder, 2019).
2. **Government Documents and Reports**: Official publications from the government agencies and institutions like the U.S government, Swedish government and relevant international bodies, such as NATO and the European Union, will be analysed on cyber power, cyber security, cyber dominance, national security and other key details related to the research. These documents will serve to provide insights into policy decisions, strategic objectives, and official narratives of states regarding cyber dominance (Bryman and Ball, 2019; Lune and Berg, 2017).

3. **Organisational Reports**: Reports from cybersecurity organisations, thought leaders, and non-governmental organisations (NGOs) will be engaged to provide data on current practices, challenges, and innovations in the field. These sources offer practical insights and complement the theoretical perspectives found in academic literature (Bryman and Ball, 2019).

3.2.2. Data Collection Period

The data collection period covers a broad historical timeframe, from the end of the Cold War to the present (1989-2024). This historical approach strives to captures the evolution of power assumptions and the development of cybersecurity strategies over time. It includes the analysis of older documents that reflect the initial stages of cybersecurity as a national security concern, as well as recent developments in cyber strategy to allow for an in-depth understanding of how past events and policies have shaped current practices within the cyberspace.

3.2.3. Geographical Scope

While the primary focus is on Sweden, comparative data from other nations will be included to contextualize Sweden's approach within a global framework. This comparative perspective helps identify unique features of Sweden's strategy and common trends in cyber dominance strategies worldwide.

3.2.4. Sources and Access

Data will be sourced from:

- **Online Databases**: Academic databases such as 'JSTOR,' 'Google Scholar,' and those of academic institutions will be used to gain access to books and journal articles.
- **Government Websites**: Government websites and portals like the official Swedish government websites, and U.S government websites among others, will be visited to secure access to relevant documents and reports for the research.
- **Organisational Websites**: Websites of cybersecurity organisations and think tanks will be used to obtain reports and publications necessary to the research.

3.3. Data Collection Methods

This research will engage two methods of Data collection and analysis, which are 'Document analysis' and 'Content analysis.'

3.3.1. Document Analysis

Morgan (2022) asserts that document analysis is a qualitative research method that involves examining various types of documents, including texts and visual materials, to understand and interpret their content and context. Similarly, Chanda (2022) advances that document analysis is particularly useful as it mostly serves as a great source of data for understanding the context and content of policies and strategies.

The steps involved in document analysis for this research include:

1. **Selection of Documents**: Identifying relevant documents, including books, journals, government reports, and organisational publications.
2. **Reading and Reviewing**: Carefully reading and reviewing the selected documents to understand the content and context.
3. **Coding and Categorizing**: Coding the data by identifying key themes, patterns, and categories.
4. **Interpreting**: Interpreting the data to draw meaningful conclusions and insights related to answering the research questions.

3.3.2. Content Analysis

Very similar to and sometimes seen as an offshoot of document analysis, content analysis is a research method used to systematically examine texts to find patterns, themes, and meanings (Chanda, 2022). This method will be used to analyse the text data from the documents which has been chosen for the research.

3.4. Justification of Methods

The chosen methods are justified based on their suitability for addressing the research questions and objectives. Document analysis is an appropriate method for this research because it allows for an in-depth examination of existing literature and official documents. This method is particularly useful for exploring historical and contextual aspects of cyber dominance strategies. It provides a comprehensive understanding of the theoretical and policy frameworks

that underpin Sweden's approach to cyber dominance (Chanda, 2022). On the other hand, content analysis is justified because it provides a systematic and replicable way to analyse textual data, helping in identifying key themes and patterns within the data which are crucial for understanding the complex nature of research topic and answering the research questions (Bryman and Bell, 2016).

3.5. Data Analysis

Thematic Analysis

Thematic analysis is used to identify, analyse, and report patterns (themes) within the data, and this process is key to this research particularly using the data collected to analyse the research topic and find answers to the research questions. Maguire and Delahunt (2017) and Naeem et al., (2023) highlights Braun and Clarke's (2006) six steps which are relevant for this research and includes:

1. **Familiarisation**: Getting familiar with the data by reading through and re-reading the documents and jotting down notes.
2. **Generating Codes**: Systematically coding relevant details and features of the data across the entire data set.
3. **Searching for Themes**: Bringing together the codes into potential themes.
4. **Reviewing Themes**: Checking if the themes work in relation to the coded extracts and the entire data set.
5. **Defining and Naming Themes**: Refining each theme and generating clear definitions and names for each theme.
6. **Producing the Report**: Producing a final report with selected extracts and analytical narrative that relate back to the research questions and literature.

Triangulation

Triangulation involves the use of multiple data sources and methods to cross-verify findings and enhance the credibility of the results. By triangulating data from books, journals, government documents, and organisational reports, the research will strive to ensure that the analysis is comprehensive and balanced. Triangulation helps to act against biases in research

while increasing the validity of the findings (Campbell et al, 2020; Vivek, Nanthagopan and Piriyatharshan, 2023).

3.6. Ethical Considerations

Since no interviews or questionnaires will be conducted, informed consent is not applicable in this research. However, ethical considerations still apply to the use of secondary data. Confidentiality is here, encompass ensuring that all data is screened rigorously to make sure that no sensitive information is disclosed. Meanwhile, government and organisational documents used in the research are publicly available and do not contain confidential information.

3.7. Limitations

Although the selected methods are appropriate for this research, there are potential limitations. First, the interpretation of themes in content analysis might be influenced by personal perspective, but this can be addressed by try as much as possible to be objective during this research process. Second, the findings from analysing Sweden's cyber strategy may not be universally applicable. However, comparing these findings with those from other countries can provide a broader understanding and increase the relevance of the results.

Chapter Four: Analysis

This chapter critically explores and interrogates the rise of cyber dominance as a national security strategy, focusing on its rise within the international system to the level where it has now become very important for states to develop in this direction, its incorporation within the national security strategies of countries, and the particular strategies Sweden has developed to ensure its continued relevance and security within the cyberspace. This chapter provides an in-depth exposition on how cyber capabilities are being incorporated by countries into their national defence frameworks and the broader implications for global security and global politics.

4.1. The Emergence of Cyber Dominance as a National Security Strategy

The concept of cyber dominance as a national security strategy has developed fast in recent years, becoming a very important part of global politics and international relations. Important figures in the national and global political environment have highlighted the peculiarity and weight of this new power dynamics domiciled in the cyberspace, such as the former president of the U.S. Barrack Obama when he remarked in an official statement that; “cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country” (The White House, 2009); President of China, Xi Jinping who contended that “without cybersecurity, there is no national security, the economy and society will not operate in a stable manner, and the broad popular masses’ interests will be difficult to guarantee” (Creemers, Triolo, and Webster, 2018); and Sweden’s minister for civil defence, Carl-Oskar Bohlin who stressed that “In the serious security policy situation, strengthening information and cybersecurity is a priority area for the government…” (NTT, 2024).

The history of cyber dominance can be traced back to the ending of the 20th century, at almost the same time when computer technologies and the internet was being developed (Reinking, and Colwell, 2015; Arctic Wolf, 2024). At first, cyber capabilities were mostly engaged as a means of gathering intelligence and a tool of electronic warfare, up till the period of the Cold War, where both the United States and the Soviet Union greatly invested in developing and acquiring technologies such as spy satelites amongst others, that could intercept and manipulate communications (Muszyński-Sulima, 2023; Leese, 2023). However, the end of the Cold War and the subsequent wide-spread of the internet brought about another great turning point.

The 21st century witnessed a geometric increase in the scope and advancement of cyberoperations, starting with the 2007 cyber-attacks on Estonia, which is widely regarded as

one of the first major instances of cyber-attack by one country against another. These attacks took place after the Estonian government moved a Soviet-era war memorial, 'the Bronze Soldier,' from a prominent location in Tallinn to a military cemetery, raising concerns mostly from the Russian-speaking population in Estonia and the Russian government (Davis, 2007; Herzog, 2011). Allegedly sponsored by the Russian government, these attacks involved DDoS attacks that crippled the government's websites, banking platforms within the country, and media websites amongst others over a period of 22 days. It succeeded in exposing the weaknesses within Estonia's critical infrastructure, seeking to undermine Estonia and the decision of its government in this case and serving as the first of many such attack that will begin to take place across the world (Ottis, 2008).

Hence, cyber dominance emerged as a very key component of national security for several reasons. One major reason is that cyber power allows countries to fight and achieve goals without having to exert more resources and financial commitment compared to traditional modes of military warfare. This is especially useful for smaller countries or groups that do not have the resources for regular military battles or the capacity to deal with much larger countries, or larger countries seeking to avoid direct confrontations. An example is the Stuxnet worm attack of the U.S. against Iran which succeeded in damaging Iran's nuclear program without the need for a traditional military strike (Lindsay, 2013), and another example, the SolarWinds hack in 2020 which was allegedly conducted by Russian state-sponsored hackers and infiltrated different U.S. federal agencies and private companies by compromising software updates, leading to data breaches and increased risks to the country's national security (Sanger 2020; Diaz, 2020).

Another key factor that led to the emergence of cyber dominance is the concern for the protection of critical infrastructure, rising in this sense as a defensive measure. The present internal structure of modern states depends greatly on digital systems for essential services such as 'energy,' 'transportation,' 'finance,' and 'healthcare' (European Parliament, 2021). Cyber-attacks on these systems can have disastrous consequences, disrupting daily life and affecting the stability of nations. In the words of Pontus Johnson, a professor at KTH Royal Institute of Technology (Sweden) and Director of the Centre for Cyber Defence and Information Security:

> ***"The threat is real…*** *The global financial system, the electricity grid, our critical infrastructure, water distribution, traffic, self-driving cars, healthcare. People can*

> *die if these systems do not function properly. The threat is palpable, and growing. That is why we need cyber defence," (CCDIS,* 2024).

Similarly, Sharma (2010) contends that the rise of cyber dominance is largely driven by the urgent need to protect critical infrastructure, making it a fundamental defensive strategy. He draws from Clausewitz's concept of war's trinity and Sun Tzu's position of how opponents should strive to win wars without fighting, to expound on the need for states to protect their digital infrastructures.

Additionally, while the era of information war is seemingly no longer as pronounced as during the period of the Cold War, it remains that it has not phased out, but has rather become more hidden and subtler due to the advancement of technology and the challenge of attribution/un-traceability that the peculiarity of this space has brought on (Simons and Lucaites, 2017; Clare and Ruhl, 2024). Through the use of digital skills, states can conduct espionage, gather sensitive information, and influence public opinion through cyber means (Li and Liu, 2021). An instance of this was in the Russian cyber interference in the 2016 U.S. elections involving the hacking of the Democratic National Committee's (NDC) servers amongst others to leak sensitive information so as to damage the reputation of certain political figures and influence voter perceptions, and also the extensive wave of social media disinformation campaigns engaged by different bots to manipulate public opinion and sow discord (ODNI, 2017; Abrams, 2019). More than this also, is the ability to influence violence actions and terrorism via the cyber space in a bid to cause widespread upheaval within adversary states (Wray, 2019; CTPN, 2022).

Activities such as this, if left unchecked has the ability to shape the geopolitical environment and affect the balance of power without having to engage in direct confrontations the states' military. Hence the ability to control and manipulate information has become a very important aspect of statecraft in this digital age (Wong, 2022; AP4D, 2024). Furthermore, cyber dominance is also a big contributing factor to deterrence and defence. By demonstrating strong cyber capabilities, states can deter potential adversaries from launching cyber-attacks, particularly because of their possessing offensive cyber capabilities which can be used to retaliate against or pre-emptively disrupt the threats of these adversaries (Iasiello, 2013; Smeets and Lin, 2018). Therefore, the integration of cyber operations into national defence strategies reflects the growing recognition of cyberspace as an important domain of warfare.

The pursuit of cyber dominance is particularly pronounced among major powers such as the United States, China, Russia, and organisations like NATO. These nations have developed and are still striving as hard to develop stronger cyber capabilities, integrating them into their broader national security frameworks. The United States, for instance, established the U.S. Cyber Command in 2009/2010, to help in defending their national interests in cyberspace and conducting offensive cyber operations when necessary (U.S. Department of Navy, 2023; Lonergan and Montgomery, 2024). China has made great moves in developing its cyber capabilities taking a stance that cyber dominance is integral to its broader strategic objectives, including economic and military development (Ball, 2011; Kolton, 2017). Russia is also known for its sophisticated cyber operations, broadly using cyber capabilities to achieve political and military goals against adversaries to influence political outcomes and project power in the global community, particularly instigating several attacks to this end (Lilly and Cheravitch, 2020; NATO, 2021). These actions, therefore, sheds light on the strategic importance of cyber dominance in modern international relations.

4.2. Critical Analysis of Sweden's Approach to Cyber Dominance

Sweden has been one of the foremost countries of the world to recognise the growing threats of the cyberspace and what it portends for stability of national security, engaging in efforts to increase its cyber capabilities and secure its cyberspace ever since the late 1900s (Bäckström, 2001; Pashkevich, Haftor, and Pashkevich, 2021). The country's approach to cyber dominance encompasses a broad and multi-level strategy which is directed towards ensuring the country's national security, economic stability, and international influence within the increasingly digital world. This approach has led the country to develop a very solid cyber framework, placing them as one of the countries of the world with the strongest cyber architecture. As of 2024, Sweden was ranked having 94.6% in the 'Global Cyber Security Index', 84.42% in the 'National Cyber Security Index,' and 95.10% in the 'Cyber Resilience Index' placing the country as the 6th country with the most solid cyber power framework (Lynn, 2024; NCSI, 2024; Techeconomy, 2024; E.U., 2024).

Consequently, reaching this level of capability over the years has been a result of rigorous incorporation of cyber development and security within their national security strategies, extensive investment in cybersecurity infrastructure, public-private partnerships, and a proactive approach to international cyber collaboration (Cyberwiser, 2021). Sweden's approach to cyber dominance can be understood in the following:

4.2.1. Incorporation within the Country's National security Strategy and Legal Systems

The Swedish government has always recognised the importance of cybersecurity and cyber dominance and the need to integrate it as part of its national security strategy and legal/regulatory framework. The national security strategy of Sweden as at 2024 embodies three focus areas; "A safe and secure Sweden, a safe, open and cohesive Sweden, and a resilient and competitive Sweden, "covering also the commitment to actively protect its national interests and defend them whenever they are threatened, including against risks and threats related to the digital arena (Government offices of Sweden, 2024b). At several instances, former Prime Minister Stefan Löfven has pointed out the need for a stronger cyber security and development for the country as a means of national security strategy and the pronounced efforts towards this end (Reuters, 2017; Government Offices of Sweden, 2021b). Meanwhile, Peter Hultqvist, Minister for Defence in 2020 remarked that: "Our security and prosperity rests on digital foundations. The ability to reap the benefits from digitalisation must be matched by an equal ability to handle the threats and risks that is part of a digital society" (Government Offices of Sweden, 2020).

Sweden's recognition of cybersecurity as a national security priority is evident in several key documents and strategic initiatives. The Swedish National Cybersecurity Strategy, introduced in 2017, clearly states that cybersecurity is very key to the protection of the critical infrastructure, economy, and societal functions of the country. Several bills and regulatory frameworks have been enacted towards this end including the 'Protective security Act of 1996,' 'Archives Act of 1990,' 'Personal Data Act of 1998' and the 'Electronic Communication Act of 2003' amongst others (Swedish Government, 2017). These laws and regulations all outlines the nature of cybersecurity practices across public and private sectors, including the requirements for regular security checks, reporting of incidences, and the adoption of best practices.

Additionally, the Swedish Civil Contingencies Agency (MSB) regularly publishes strategic documents and reports that sheds light on the priorities and actions of the country for cybersecurity, for example, its 2019 report "Comprehensive cyber security action plan 2019–2022" which provided an expansive overview of the strategic initiatives and measures taken to enhance national cybersecurity (MSB, 2019). These conversations and documents serve as a blueprint for reinstating the pertinence of cyber dominance efforts and consequently helping to integrate cybersecurity into national security policies and ensuring that Sweden's responses to

cyber threats and cyber development are coordinated, effective and bound within certain confines of laws and regulations, particularly for the private sphere.

4.2.2. Advancing Cyber Capabilities

To maintain and enhance its cyber dominance, Sweden invests heavily in building advanced cyber capabilities. In the early 2000s, the country's efforts in cyberspace were focused towards developing resilience and defensive measures as it held strongly to its stance on neutrality and diplomacy in its interrelations with other countries the international system (Lundmark, 2021; Brommesson, Ekengren, and Michalski 2022). Over the years, The Swedish National Cybersecurity Strategy in conjunction with the Swedish Civil Contingencies Agency has embodied these efforts, both those within Sweden and outside the country (Swedish Government, 2017; MSB, 2019). Additionally, the Swedish National Defense Radio Establishment (FRA) which has been in operations since the World War II was expanded from merely intercepting radio signals to sift out enemy interference, to actively contributing to the improvement of the country's cyber defences. This included them conducting security tests on government systems and monitoring communications to detect external threats, strengthened by increased funding in response to tensions in the region (Cederberg, 2018).

However, in recent years, Sweden has begun to increase focus on developing more robust defence and increasing its offensive capabilities in the cyberspace. The Swedish Armed Forces has integrated cyber capabilities into their operational framework, supported by the Cyber Defence Unit within the Swedish military. The Swedish Defence Commission submitted an extensive report towards the development of a robust offensive mechanism as with defensive, highlighting the growing capabilities of other countries including China and Russia, and the need for cooperation amongst the Armed forces and other agencies like the National Defence Radio Establishment (FRA), the Swedish Security Service and the Swedish Civil Contingencies Agency (MSB) (The Swedish Defence Commission, 2020). Subsequently, this development of offensive capabilities began in the 2020 with the passing of the 'Total Defence Bill' by the parliament in December 2020, and more so in 2022 with the creation of new cyber units called 'ITF and 2ITF,' and the increased efforts towards recruiting people to this end (Shephard, 2022; Swedish Armed Forces, 2023).

Staring from 2019, the country has undertaken several exercises including the SAFE Cyber 2019 exercise held by the Swedish Armed Forces involving public authorities and companies related to cybersecurity and the military's systems, and the Total Defence Exercise 2020, which also included extensive cyber defence exercises. These exercises simulated large-scale

cyberattacks on critical infrastructure and tested the coordination between military and civilian agencies in responding to such threats (MBS, 2020a; MSB, 2020b). Much emphasis is placed on these exercises and coordination between all the relevant units in the country, even to the extent of thoroughly screening partnerships with private organisations to ensure little or no gaps within the country's cyber system (Cederberg, 2018; MSB, 2020a). Meanwhile the government has also invested a lot of finances into cyber development, with Sweden's 2023 draft budget bringing in an increase of $1.23 billion in defence and national security spending, with a focus on enhancing cyber defence capabilities to meet NATO's spending targets, bolster Sweden's defence infrastructure and protect critical infrastructure (O'Dwyer, 2022).

Asides military methods of advancing the country's cyber capabilities, Sweden also integrates efforts in education, research, and innovation to further advance the development of its cybersecurity (Government Offices of Sweden, 2024b). Cybersecurity is embedded into the curriculum of schools in the country, seeking to teach students computer skills and how to recognise fake news and disinformation, and specialised training programs engaged to cultivate a skilled future workforce capable of tackling these future threats (Cederberg, 2018). Concurrently, Sweden, particularly through the Swedish Armed Forces invests in research and development, particularly in advanced fields like artificial intelligence and machine learning, in a bid to spark innovation and enhance its threat detection and response capabilities (MSB, 2020a). The various public awareness campaigns undertaken by the government, Armed forces and other agencies also further complement these efforts by educating citizens on safe online practices, thereby developing a culture of security and resilience throughout society (Swedish Government, 2017; MSB, 2020a). These broad measures towards advancing the country's cyber capabilities not only strengthen Sweden's immediate cybersecurity posture, but they also serve to ensure long-term national resilience in the face of the ever-changing cyber threats.

4.2.3. International Collaboration

Over the years, Sweden's policy of neutrality and diplomacy has positioned it as a core player in global cyber cooperation, as it strives to protect its interest while also strengthening its defences (Cederberg, 2018). The need for international collaborations is strongly recognised by the government and is a main feature of the Swedish National Cybersecurity Strategy which highlights that "International cooperation on cyber security is to be enhanced, as part of the objective of a global, accessible, open and robust internet characterised by freedom and respect for human rights" (Swedish Government, 2017). Hence, they have always been focused on collaborations within the European Union, as also shed light upon in the Total Defence bill,

which advances that "the EU is Sweden's most important platform for foreign and security policy. It is in Sweden's national interest to safeguard and strengthen the EU's cohesion, cooperation, solidarity, and integration" (The Swedish Defence Commission, 2020). This assertion influences and embodies Sweden's commitment to participating in and reinforcing collective security measures, as relating to cybersecurity and its pursuit of cyber power in the international system.

As part of the European Union, Sweden complies with the Network and Information Security (NIS) Directive, developed in 2016, and then updated in 2023, which calls for high security standards for network and information systems among member states so as to enhance overall resilience of cybersecurity and response capabilities (European Commission, 2023). Sweden actively participates in EU cybersecurity initiatives, contributing to the development of policies such as "EU's Customs Information Systems, the Decision of the Council on the establishment of the EU Agency for law enforcement cooperation (Europol), the Regulation concerning the Visa Information System (VIS Regulation) and the Regulation on the establishment of EURODAC (EURODAC Regulation)" (European Commission, 2024). For about 30 years now, Sweden has engaged in a close partnership with NATO for many security matters including Cyber Security, starting from 1994 when the country joined the Partnership for Peace (PfP) program. The country has participated in several missions led by NATO including the Resolute Support Mission in Afghanistan, the Kosovo Force (KFOR) in Kosovo, and several other Cyber Coalition exercises up until they officially joined the organisation in March 7, 2024 (NATO, 2024)

Additionally, Sweden has formed numerous partnerships with other countries, especially with its immediate neighbours to enhance its cyber defence capabilities. One of these partnerships is the Nordic Defence Cooperation (NORDEFCO) established in 2009 with Denmark, Finland, Iceland, and Norway to enhance their regional security and develop their military capabilities through joint training, procurement, and other joint efforts so as to deter Russia's aggressive moves within the region (Dahl, 2021). In April 2024, Sweden also entered an agreement with the United States European Command (USEUCOM), signing a bilateral Letter of Intent (LOI) to set up a framework for cyber cooperation which focuses on policy, training, capability development, and cyber operations between both countries (Swedish Armed Forces Headquarters, 2024). Consequently, Sweden has been and is still pulling all stops to increase its cyber capabilities via cooperating with other countries and organisations.

4.2.4. Public-Private Cooperation

Sweden, as a country, recognises that a great portion of critical infrastructure and digital development lies within the private sector and its citizens who are mostly digitally inclined are susceptible to different cyber threats and vulnerabilities. To this end, the country engages in partnership with private entities (Swedish Government, 2017). The Swedish Civil Contingencies Agency (MSB) plays an important role in coordinating cybersecurity between the government and private sector. It provides advice, resources, and support to strengthen the security of critical infrastructure. The agency also helps to share information and promote teamwork among government agencies, private companies, and universities so as to institutionalise best practices and assist them in understanding threats and responding to incidents (MSB, 2020b; Cyberwiser, 2021).

4.3. Sweden and Global Implications of Cyber Dominance

The emergence of cyber power and cyber dominance in global politics and as an integral part of national security strategy of countries has brough about several implications within the international system. These implications and changes include its reflections on power dynamics in the international system, its influence in political, social and economic spheres of nations, and ethical and legal considerations arising from the engagement of this space as expounded below:

4.3.1. Influence on Global Power Dynamics

The emergence of cyber dominance is reshaping the nature of power dynamics and the national security strategies of countries across the globe. Traditionally, power in the international system has been measured through military, economic, and political might, but the digital age has brought cyber capabilities to the fore of being very important part of a nation's power (Nye, 2010). Cyber dominance allows states to reflect great influence in the international system and project power without facing the costs and risks associated with conventional military engagements. This shift in power dynamics and need for cyber dominance is vividly seen in how major powers are increasingly prioritising cyber capabilities (Voo et al, 2020; IISS, 2023). Sweden, for example, has recognised the strategic importance of cyber dominance and has integrated it into its national security strategy, with its National Cybersecurity Strategy emphasising the importance of robust cyber defences and offensive capabilities to protect

national interests and project power in the international arena (Swedish Government, 2017). Similarly, this is the same for major powers including the U.S, Russia, and China (IISS, 2023).

The pursuit of cyber dominance by one state frequently leads to responses and adjustments from other states, creating a constantly changing environment of cyber capabilities and cyber power tussles. As countries recognise the many benefits of having cyber dominance, they begin to invest a lot of resources in strengthening their own cyber capabilities both as an instrument of defence and also one for offence (Healey and Jervis, 2020; Mishra et al, 2022). For instance, the early 2000s witnessed a lot of aggressive cyber activities from Russia including Estonia and Georgia cyberattacks in 2007 and 2008 respectively, and several other espionage and influencing operations, causing the U.S to establish its Cyber Command in 2010 to defend its national security in the cyber space (Deppa, 2017; Matishak, 2018; Odoh, 2021). China, has also rapidly expanded its cyber capabilities in recent years focusing on cyber espionage and theft of intellectual property, as well as on developing the capacity to disrupt the critical infrastructures of its adversaries within the international system (Sebenius, 2023; IISS, 2023).

Meanwhile, Sweden is not left out of this pursuit for cyber dominance, as the country has had to revise its strategies over the years, from the development of a National Cybersecurity Strategy in 2017, to the incorporation the need to advance cyber capabilities in the Total Defence bill in 2020 (Swedish Government, 2017; Swedish Armed Forces, 2023). Despite striving to maintain its renowned neutrality within the region, the need for developing its cyber capabilities amongst others has incessantly caused Sweden to Partner with NATO over the years (NATO, 2024). Hence, power struggles in the international system have shifted from a total focus on physical military capabilities, having states striving for increased cyber capabilities as a form of power.

4.3.2. A Tool for Political and Economic Leverage

Cyber dominance is increasingly accepted as a key instrument for helping countries achieve both political leverage and economic advantage. Through the use of the cyberspace, states are able to impact the political environment of other nations, protect their own economic interests, and destabilise those of other countries (IISS, 2023). An example of the reflection of cyber dominance as a political tool is the alleged interference of Russian hackers and its impact on the 2016 United States presidential election. The goal of this incidence was not just to influence the outcome of the election, but also to negatively affect the confidence of the public in the existing democratic institutions and processes in the United States, create confusion and

division (Nakashima and Harris, 2018; Bandurski, 2022). However, such interference is not limited to the United States but other various countries, including Sweden who have reported similar incidents such as when the former prime minister, Stefan Löfven spoke strongly against foreign influence in Sweden's election process (The Local, 2017).

Moreover, cyber dominance allows for the use of sophisticated propaganda and misinformation campaigns. These campaigns can spread rapidly through social media and other digital platforms, reaching a wide audience very fast and controlling or influencing narratives on such a scale that it can shape public opinions and policies in other countries (EPRS, 2019; Bandurski, 2022). This is particularly concerning as it reveals a form of hybrid warfare wherein cyber operations are combined with conventional military tactics to achieve strategic objectives without direct a need for confrontation. Cyber dominance also allows states to conduct industrial espionage and sabotage on physical infrastructures. The Stuxnet virus, discovered in 2010 and allegedly developed by the United States, is a well-known case where a cyber weapon was used to damage Iran's nuclear centrifuges (Hayward, 2017). This attack set back Iran's nuclear program by several years without the need for a traditional military strike.

Economically, cyber dominance enables countries to engage in activities that can significantly impact global economic balances. One prominent example is the theft of intellectual property and trade secrets. Countries like China engage in orchestrating widespread cyber espionage campaigns targeting corporations and other institutions in order to gain access to important technologies and business information so accrue competitive edge in global markets or to cause financial losses for the targeted companies and countries (Rugina, 2023). Meanwhile, another aspect of the economic dimension is the ability to use cyber-attacks to destabilise financial systems. The financial sector is has grown to become reliant on the digital space, with the rise of cryptocurrencies and digital financial technologies adding more to this complexity and increasing its vulnerabilities. Attacks on financial institutions can lead to data breaches, financial theft, disruption of services, loss of trust in financial systems, and even broader economic instability (Jiang and Broby, 2021; IMF, 2021). Also, by threatening or actually disrupting critical infrastructure, such as energy grids or communication networks, states can exert pressure on others to comply with their demands (UNOCT, 2022).

Over the years, Sweden has made use of its advanced cybersecurity capabilities to influence polices in the European Union, calling for more stringent cybersecurity measures. While the country is not focused on cyber espionage and the influencing or disruption of the critical infrastructure of other nations, Sweden positions itself as a leader in shaping cybersecurity

norms and standards in the international system (The Swedish Defence Commission, 2020; European Commission, 2024).

4.4. Ethical and Legal Considerations

The pursuit of cyber dominance brings about different ethical and legal challenges due to the peculiarities of cyber capabilities and its existence within cyberspace which is mostly unregulated (Katagiri, 2021). One major legal issue is the difficulty in accurately attributing cyber-attacks, as perpetrators can act in secrecy, complicating the enforcement of international laws regarding sovereignty and non-intervention. Unlike conventional military actions, cyber-attacks can help nations and attackers to cross borders without physically entering adversary nations, raising questions about violations of sovereignty and the principle of non-intervention, which prohibits states from interfering in other states' internal affairs (Moynihan, 2019). Also, there are challenges in applying the concept of proportionality in cyber warfare, as the impacts can be widespread and unpredictable, affecting both civilians alongside military targets (Pascucci, 2017; Katagiri, 2021).

Ethically, cyber capabilities present moral dilemmas, such as adverse impacts on civilian populations when critical infrastructure is targeted and essential services like electricity, water, and healthcare are disrupted. These actions raise serious ethical questions about how cyber activities can harm innocent citizens and impact the stability of societies (Husch and Lahmann, 2022). Moreover, extensive surveillance and data collection in cyber operations can infringe on privacy and human rights, posing a challenge on how to go about balancing national security with individual rights (Allahrakha, 2023). Sweden to this end has developed several internal policies and bills including the ‘Protective Security Act of 1996, ‘Personal Data Act of 1998’ and the ‘Electronic Communication Act of 2003’ amongst others, and also engaging with the international community to create a semblance of guiding principles to secure the cyberspace (Swedish Government, 2017).

Chapter Five: Conclusion

The central puzzle which led to the carrying out of this study was the peculiarities of cyber capabilities and its relevance to global politics and power struggle in the international system. This study sought to interrogate the development of cyber capabilities within the international system to a level where it is now ascribed as a form of power, how these capabilities are integrated into national security strategies of countries, and what this means for international relations and global security. To this end, this study examined the strategies used by the Swedish government to shed more light into how countries are adapting to the race for cyber dominance and the ever-changing nature of threats in the digital age.

The central argument of this dissertation is that cyber dominance has come to be integral part of national security strategy of countries across the world. However, Sweden's approach to cyber dominance reflects a focused and proactive stance in safeguarding national security, as the country have developed a broad cyber strategy that combines cyber capabilities with traditional security measures. To investigate this argument, the study examined the historical assumptions of power and how these assumptions have been confronted and impacted by the development of cyber power. It analysed Sweden's security policies over the years, expounding on how these policies have been updated and reformed to address the growing cyber threats in the international system. The study also provided a thorough understanding of the approach of Sweden towards cyber dominance and development and its implications.

One of the key findings of this research is that Sweden's cyber strategy places strong emphasis on resilience and collaboration, investing in both defensive and offensive cyber capabilities. These efforts are aimed at protecting the nation's critical infrastructure while also making them prepared for potential cyber conflicts. The country has also and is still partnering with other countries and organisations including the United States, NATO and the EU to increase its cyber capabilities.

The contribution of this thesis to the field of Global Politics lies in its detailed examination of how cyber dominance is shaping both the concept of power in the international system and national security strategies of countries. By focusing on Sweden, this study has provided a case study that reveals broader trends in cybersecurity and national security and a deep understanding towards the dynamics of cyber power and its impact on global security. However, while the research has provided greats insights, it is also important to bring to light the limitations of this study. The focus on Sweden, while providing a detailed case study, may not fully capture the diversity of approaches engaged by other nations to deal with cyber threats

and strive towards cyber dominance. Consequently, further research could expand the scope to include comparisons with other countries and examine how their different strategies as relating to cyber dominance can have a marked impact on global power struggles and security.

References

Abrams, Abigail (2019) 'Here's What We Know So Far About Russia's 2016 Meddling'. *Time*. Online: https://time.com/5565991/russia-influence-2016-election/ (Accessed: 19 July 2024).

Ackerman, Robert (2021) *'Government and Private Sector Cybersecurity Collaboration Finally Showing Signs of Life'.* Available at: https://www.rsaconference.com/library/blog/government-and-private-sector-cybersecurity-collaboration-finally-showing-signs-of-life (Accessed: 03 July 2024)

Ainslie, Scott, Thompson, Dean, Maynard, Sean, and Ahmad, Atif (2023) 'Cyber-threat intelligence for security decision-making: A review and research agenda for practice', *Computers & Security*, 132.

Al-Tae, Asmaa Khalid Jarjees, Al-Dhalimi, Hameeda Abdul-Hussain, and Al-Shaibani, Adnan KadhumJabbar (2020) 'Relationship of Cybersecurity and the National Security of the Country: Iraq Case Study', *Systematic Reviews in Pharmacy,* 11 (12), pp. 469-476.

Allahrakha, Naeem (2023) 'Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age', *Legal Issues in the Digital Age*, 4(2), pp. 78–121.

Antunes, Sandrina and Camisão, Isabel (2018) 'Introducing Realism in International Relations Theory', *E-International Relations*, February 27. Online: https://www.e-ir.info/2018/02/27/introducing-realism-in-international-relations-theory/ (Last accessed: 10 July 2024).

Arctic Wolf (2024) *'A Brief History of Cybercrime'.* Online: https://arcticwolf.com/resources/blog/decade-of-cybercrime/ (Accessed: 19 July 2024).

Asia-Pacific Development, Diplomacy & Defence Dialogue (AP4D) (2024) *What does it look like for Australia to Use All Tools of Statecraft in the Information Environment*. Asia-Pacific Development, Diplomacy & Defence Dialogue.

Bäckström, Urban (2001) *Sweden's economy and new information technology.* Online: https://www.bis.org/review/r010212a.pdf (Last accessed: 04 July 2024).

Bailes, Alyson J. K., Herolf, Gunilla, and Sundelius, Bengt (eds.) (2006) *The Nordic Countries and the European Security and Defence Policy* (New York: Oxford University Press).

Ball, Desmond (2011) 'China's Cyber Warfare Capabilities', *Security Challenges,* 7(2), pp. 81–103.

Bandurski, David (2022) 'China and Russia are joining forces to spread disinformation', *Brookings.* Online: https://www.brookings.edu/articles/china-and-russia-are-joining-forces-to-spread-disinformation/ (Accessed: 29 June 2024).

Biller, Jeffrey T., and Schmitt, Michael N. (2019) 'Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare', *International Law Studies*, (95), pp. 179-225.

Brommesson, Douglas, Ann-Marie Ekengren, and Anna Michalski (2022) *'Sweden's Policy of Neutrality: Success Through Flexibility?',* in Caroline de la Porte et al. (eds), *Successful Public Policy in the Nordic Countries: Cases, Lessons, Challenges* (Oxford: Oxford Academic)

Bryant, Rebecca (2001) 'What Kind of Space is Cyberspace?', *Minerva - An Internet Journal of Philosophy,* 5, pp. 138-155.

Bryman, Alan and Bell, Edward (2019) *Social Research Methods*. Ontario: Oxford University Press.

Burlacu, Sorin, Oancea Negescu, Mihaela Diana, Patarlageanu, Simona Roxana, and Vasilescu, Raluca Ana (2021) 'Digital globalization and its impact on economic and social life', *SHS Web of Conferences 129*, 06003.

Campbell, R., Goodman-Williams, R., Feeney, H., and Fehler-Cabral, G. (2020) 'Assessing Triangulation Across Methodologies, Methods, and Stakeholder Groups: The Joys, Woes, and Politics of Interpreting Convergent and Divergent Data'*, American Journal of Evaluation*, 41 (1), pp.125-144.

Canfil, Justin (2022) 'The illogic of plausible deniability: why proxy conflict in cyberspace may no longer pay,' *Journal of Cybersecurity*, 8(1), tyac007.

Carr, Madeline, and Nye, Joseph (2018) 'From Nuclear Weapons to Cyber Security: Breaking Boundaries', (in Springer eBooks), pp. 87-96.

Cavelty, Dunn M., and Wenger, Andreas (eds.) (2022) *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation* (Milton Park: Routledge).

Cederberg, Gabriel (2018) *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections*. Online: https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf (Accessed: 20 July 2024).

Centre for Cyber Defence and Information Security (CCDIS) (2024) 'The threat is real'. Online: https://www.kth.se/cdis (Accessed: 19 July 2024).

Chanda, A. (2021) 'Key methods used in qualitative document analysis,' *Social Science Research Network* [Preprint].

Chin, John J., Skinner, Kiron, and Yoo, Clay (2024) 'Understanding National Security Strategies Through Time', *The Strategist*, 4(6), pp. 103-124.

Chin, Warren (2019) 'Technology, war and the state: past, present and future', *International Affairs,* 95(4), pp. 765-783.

Clare, Stephen and Ruhl, Christian (2024) 'A New Cold War Could End Civilization — without Turning Hot: How Should US-China Technology Competition Be Managed in the Twenty-First Century?'. *Center for International Governance Innovation*. Online: https://www.cigionline.org/articles/a-new-cold-war-could-end-civilization-without-turning-hot/ (Accessed: 19 July 2024).

Counter Terrorism Preparedness Network (CTPN) (2022) *City Preparedness for Cyber-Enabled Terrorism – Report 2022*. London: CTPN.

Creemers, Rogier, Triolo, Paul, and Webster, Graham (2018) 'Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference'. Online: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/ (Accessed: 19 July 2024).

Creswell, J.W. and Poth, C.N. (2018) *Qualitative Inquiry and Research Design Choosing among Five Approaches,* (SAGE Publications, Inc., Thousand Oaks).

Cristiano, Fabio, and van den Berg, Bibi (eds.) (2023) *Hybridity, Conflict, and the Global Politics of Cybersecurity* (Lanham: Rowman & Littlefield).

Cronberg, Tarja (2008) *The Will to Defend: A Nordic Divide over Security and Defence Policy.* Online: https://www.sipri.org/sites/default/files/files/books/SIPRI06BaHeSu/SIPRI06BaHeSu18.pdf (Last accessed: 04 July 2024).

Cybersecurity and Infrastructure Security Agency (CISA, US) (2023) '*The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years'*. Available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years (Accessed: 03 July 2024).

Cybersecurity and Infrastructure Security Agency (CISA, US) (2024) '*Partnerships and Collaboration'*. Available at: https://www.cisa.gov/topics/partnerships-and-collaboration (Accessed: 03 July 2024)

Cyberwiser (2021) *Sweden (SE).* Online: https://cyberwiser.eu/sweden-se (Last accessed: 03 July 2024).

Dahl, Ann-Sofie (2021) 'Back to the Future: Nordefco's First Decade and Prospects for the Next', *Scandinavian Journal of Military Studies*, 4(1), pp. 172–182.

Davis, Joshua (2007) 'Hackers Take Down the Most Wired Country in Europe'. *Wired*. Available at: https://www.wired.com/2007/08/ff-estonia/ (Accessed: 19 July 2024).

Deppa, Catherine S. (2017) 'U.S. Cyber Command: An Overview', *American Intelligence Journal*, 34(1), pp. 12–15.

Diaz, Jaclyn (2020) 'Russia Suspected In Major Cyberattack On U.S. Government Departments'. *NPR*. Online: https://www.npr.org/2020/12/14/946163194/russia-suspected-in-months-long-cyber-attack-on-federal-agencies (Accessed: 19 July 2024).

Doshi, Rush, and Williams, Robert D. (October 2, 2018) 'Is China interfering in American politics?', *Brookings*. Online: https://www.brookings.edu/articles/is-china-interfering-in-american-politics/ (Accessed: 29 June 2024).

Duguin, Stéphane and Pavlova, Pavlina (2023) 'The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict', *European Union*. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf (Accessed: 03 July 2024)

Dunn, David Hastings (2007) 'Real men want to go to Tehran": Bush, pre-emption and the Iranian nuclear challenge', *International Affairs*, 83(1), pp. 19-38.

ECDPM (2017) *What we can learn from Sweden on promoting sustainable peace.* Online: https://ecdpm.org/work/what-we-can-learn-from-sweden-on-promoting-sustainable-peace (Last accessed:04 July 2024).

Edler, Jakob, Blind, Knut, Kroll, Henning, and Schubert, Torben (2023) 'Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means', *Research Policy,* 52(6).

Edwards, Christian, Hansler, Jennifer, and Knight, Mariya (07/03/2024) 'Sweden officially joins NATO, becoming alliance's 32nd member'. *CNN*. Available at: https://edition.cnn.com/2024/03/07/europe/sweden-join-nato-official-intl/index.html (Accessed: 04 July 2024).

EU CyberNet (2023) *'The EU's International Cooperation on Cyber Capacity Building'* (Tallinn: EU CyberNet).

European Commission (2023) 'Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)'. Online: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (Accessed: 20 July 2024).

European Commission (2024) SWEDEN 2024: Digital Public Administration Factsheet. Online: https://joinup.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Sweden_vFinal.pdf (Accessed: 20 July 2024).

European Parliament (2021) 'Cybersecurity: why reducing the cost of cyberattacks matters'. Online: https://www.europarl.europa.eu/topics/en/article/20211008STO14521/cybersecurity-why-reducing-the-cost-of-cyberattacks-matters (Accessed: 19 July 2024).

European Parliamentary Research Service (EPRS) (2019) *Polarisation and the use of technology in political campaigns and communication*. European Parliament.

Futter, Andrew (2016) 'Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy', *Royal United Services Institute (RUSI) Occasional Paper,* (Whitehall: Royal United Services Institute for Defence and Security Studies).

Geers, Kenneth (2009) 'The Cyber Threat to National Critical Infrastructures: Beyond Theory', *Information Security Journal: A Global Perspective*, 18:1–7.

Gilad, Amitai, Pecht, Eyal, and Tishler, Asher (2020) 'Intelligence, cyberspace, and national security,' *Defence and Peace Economics*, 32(1), pp. 18–45.

Government Offices of Sweden (2020) *Speech by Minister for Defence Peter Hultqvist at Hanating, 17 November 2020*. Online: https://www.government.se/contentassets/b76ad79ca1fc4cdf91920c2688b50bdc/minister-for-defence-peter-hultqvist-speeches-2014-2022.pdf (Accessed: 20 July 2024).

Government Offices of Sweden (2021a) *National Security Strategy.* Online: https://www.almendron.com/tribuna/wp-content/uploads/2021/01/national-security-strategy.pdf (Last accessed: 04 July 2024).

Government Offices of Sweden (2021b) *Speech by Prime Minister Stefan Löfven at UN Climate Change Conference COP26*. Online: https://www.government.se/contentassets/4613e972fd8240429069440b70e2c909/prime-minister-stefan-lofven-speeches-2014-2021.pdf (Accessed: 27 July 2024).

Government Offices of Sweden (2024a) '*Why Sweden joined NATO - a paradigm shift in Sweden's foreign and security policy'.* Available at: https://www.government.se/speeches/2024/04/why-sweden-joined-nato---a-paradigm-shift-in-swedens-foreign-and-security-policy/ (Accessed: 04 July 2024).

Government Offices of Sweden (2024b) *National Security Strategy*. Stockholm: Government Offices of Sweden.

Handler, Simon (2022) '*The 5×5—Non-state armed groups in cyber conflict'*. Available at: https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-non-state-armed-groups-in-cyber-conflict/ (Accessed: 03 July 2024)

Hayward, Ryan J. (2017) 'Evaluating The "Imminence" Of A Cyber Attack for Purposes of Anticipatory Self-Defense', *Columbia Law Review,* 117(2).

Healey, Jason and Jervis, Robert (2020) 'The Escalation Inversion and Other Oddities of Situational Cyber Stability', *Texas National Security Review*, 3(4), Fall, pp. 1-20.

Herzog, Stephen (2011) 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses', *Journal of Strategic Security*, 4(2), pp. 49–60.

HM Government (2022) *National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK.* Online: https://assets.publishing.service.gov.uk/media/620131fdd3bf7f78e469ce00/national-cyber-strategy-amend.pdf (Last accessed: 03 July 2024).

Holmes, Kim R. (2015) *'What Is National Security?* Available at: https://www.heritage.org/sites/default/files/2019-10/2015_IndexOfUSMilitaryStrength_What%20Is%20National%20Security.pdf (Accessed: 03 July 2024)

Husch, Pia and Lahmann, Henning (2022) 'Societal Risks and Potential Humanitarian Impact of Cyber Operations'. Online: https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Societal%20Risks%20and%20Potential.pdf (Accessed: 27 July 2024).

Iasiello, Emilio (2013) 'Is Cyber Deterrence an Illusory Course of Action?', *Journal of Strategic Security*, 7(1), pp. 54-67.

Iftikhar, S. (2024) 'Cyberterrorism as a global threat: a review on repercussions and countermeasures', *PeerJ Comput Sci*, 10, e1772.

Informationsverige (2023) *The history of Sweden*. Online: https://www.informationsverige.se/en/om-sverige/att-komma-till-sverige/sveriges-historia.html (Last accessed: 04 July 2024).

International Monetary Fund (IMF) (2021) 'The Global Cyber Threat', Finance & Development, pp. 24–27.

International Trade Administration (ITA) (2023) 'Cybersecurity', Online: https://www.trade.gov/country-commercial-guides/sweden-cybersecurity (Accessed: 28 June 2024).

Jensen, Benjamin (2017) 'The Cyber Character of Political Warfare', *The Brown Journal of World Affairs*, vol. 24, no. 1, pp. 159–172.

Jewish Institute for National Security of America—JINSA (2023) '*No Daylight: U.S. Strategy if Israel Attacks Iran'*. Available at: https://jinsa.org/wp-content/uploads/2023/07/JINSA_Report_No-Daylight-1.pdf (Accessed: 03 July 2024)

Jiang, Chenle and Broby, Daniel (2021) 'Mitigating Cybersecurity Challenges in the Financial Sector with Artificial Intelligence'. Centre for Financial Regulation and Innovation.

Jonasson, Axel E. (1973) 'The Crimean War, the Beginning of Strict Swedish Neutrality, and the Myth of Swedish Intervention in the Baltic', *Journal of Baltic Studies*, (4:3), pp. 244-253.

Kala, Emile S. (2023) 'Critical Role of Cyber Security in Global Economy', *Open Journal of Safety Science and Technology*, 13(4), pp. 231-248.

Kaspersky. 2021. DarkChronicles: the consequences of the Colonial Pipeline attack. https://ics-cert.kaspersky.com/publications/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/#:~:text=a%20single%20incident.-,Attack%20on%20Colonial%20Pipeline,a%20cyberattack%20involving%20DarkSide%20ransomware (Accessed: 03 July 2024).

Katagiri, Nori (2021) 'Why international law and norms do little in preventing non-state cyber attacks', *Journal of Cybersecurity*, 7(1).

Keohane, Robert O., and Nye, Joseph S. (1998) 'Power and Interdependence in the Information Age', *Foreign Affairs*, 77(5), pp. 81-94.

Khanday, Sumbl Ahmad and Khanam, Deeba (2019) 'The Research Design', *Journal of Critical Reviews*, (6:3), pp.367-376.

Kiderlin, Sophie (2024) 'Sweden formally joins NATO military alliance, ending centuries of neutrality'. *CNBC*. Available at: https://www.cnbc.com/2024/03/07/sweden-formally-joins-nato-military-alliance-ending-decades-of-neutrality.html (Accessed: 04 July 2024).

Kolton, Major Michael (2017) 'Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence', The Cyber Defense Review, 2(2), pp. 119–153.

Kramer, Franklin D., Starr, Stuart H., Wentz, Larry, and Zimet, Elihu (2007) "Adapting C2 to the 21st Century": Frameworks and Insights Characterizing Trends in Cyberspace and Cyberpower. In: *Proceedings of the 12th ICCRTS, Track: C2 Concepts, Theory, and Policy.* Online: http://www.dodccrp.org/events/12th_ICCRTS/CD/html/papers/165.pdf (Accessed: 02 July 2024).

Krebs, R.R. (2018) 'The Politics of National Security,' *The Oxford Handbook of International Security*, pp. 258–273.

Kuehl, Daniel T. (2009) *Cyberpower and National Security*. Potomac Books, University of Nebraska Press.

L.A Times (1989) 'Reagan urges 'Risk' on Gorbachev : Soviet leader may be only hope for change, he says,' *Los Angeles Times*, 13 March. https://www.latimes.com/archives/la-xpm-1989-06-13-mn-2300-story.html. (Last accessed: 28 June 2024).

Leese, Bryan (2023) 'The Cold War Computer Arms Race', *Journal of Advanced Military Studies*, 14(2), pp. 102–120.

Lewis, James A. (2020) 'A Necessary Contest: An Overview of U.S. Cyber Capabilities', *Asia Policy*, 15(2), pp. 84-92.

Lonergan, Erica (2024) *'United States Cyber Force: A Defense Imperative', Columbia University.* Available at: https://www.fdd.org/analysis/2024/03/25/united-states-cyber-force/ (Accessed: 03 July 2024)

Li, Yuchong, and Liu, Qinghui (2021) 'A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments', *Energy Reports*, (7), pp. 8176-8186.

Lilly, Bilyana and Cheravitch, Joe (2020) 'The Past, Present, and Future of Russia's Cyber Strategy and Forces', in Jančárková, T., Lindström, L., Signoretti, M., Tolga, I., and Visky, G. (eds.) *The Next Decade.* NATO CCDCOE Publications, Tallinn.

Lindsay, Jon R. (2013) 'Stuxnet and the Limits of Cyber Warfare', *Security Studies,* 22(3), pp. 365–404.

Liu, Zongyi (2014) '*The Concept of National Interests'*, in China's Diplomacy (World Century Publishing Corporation), pp. 121-189.

Lundmark, Martin (2021) 'The Evolution Towards the Partial Strategic Autonomy of Sweden's Essential Security Interests', *Defence and Peace Economics*, 33(4), pp. 399–420.

Lune, Howard and Berg, Bruce L. (2017) *Qualitative Research Methods for the Social Sciences* (Edinburgh Gate: Pearson Education Limited).

Lynn, Samara (2024) 'Countries With The Highest Cyber Threat Risk And Ones With The Lowest: Report'. Online: https://www.mescomputing.com/news/4208968/countries-cyber-threat-risk-ones-lowest-report (Accessed: 20 July 2024).

Maguire, Moira and Delahunt, Brid (2017) 'Doing a Thematic Analysis: A Practical, Step-by-Step Guide for Learning and Teaching Scholars', AISHE-J, 3, Autumn, pp. 33501-33514.

Makko, Aryo (2012) 'Sweden, Europe, and the Cold War: A Reappraisal', *Journal of Cold War Studies*, (14:2), pp. 68-97.

Malik, Jitender K., and Choudhury, Sanjaya (2019) 'Cyber Space - Evolution and Growth', *East African Scholars Journal of Education, Humanities and Literature*, 2(3), pp. 170-190.

Martino, Luigi (November 13, 2023) 'At the Space and Cyber Intersection: Geopolitical Implications and Power Effects', *Italian Institute for International Political Studies*. Online: https://www.ispionline.it/en/publication/at-the-space-and-cyber-intersection-geopolitical-implications-and-power-effects-153095 (Last accessed: 30 June 2024).

Marzagalli, Silvia and Müller, Leos (2016) 'In apparent disagreement with all law of nations in the world: Negotiating neutrality for shipping and trade during the French Revolutionary and Napoleonic Wars', *International Journal of Maritime History*, 28(1), pp. 108-117.

Matishak, Martin (2018) ‘A decade after Russia hacked the Pentagon, Trump unshackles Cyber Command’. *Politico*. Online: https://www.politico.com/story/2018/11/29/a-decade-after-russia-hacked-the-pentagon-trump-unshackles-cyber-command-961103 (Accessed: 26 July 2024).

McFarland, Conor (2011) ‘Cyber Warfare: Explaining the Absence of Physical Force Responses by States.’ *Undergraduate Theses and Capstone Projects*, 91. Available at: https://digitalshowcase.lynchburg.edu/utcp/91 (Accessed: 03 July 2024).

McNeilly, Mark (2015) *'Deception and Foreknowledge: Winning the Information War'*, in Sun Tzu and the Art of Modern Warfare (New York: Oxford Academic).

Meierding, Emily and Sigman, Rachel (2021) ‘Understanding the Mechanisms of International Influence in an Era of Great Power Competition’, *Journal of Global Security Studies*, (6:4), ogab011.

Milante, Gary, Lilja, Jannie, Kluyskens, Jups, and Lindström, Johanna (2021) Practicing Peacebuilding Principles: A Study of Sweden’s Engagement with Fragile and Conflict-Affected States, *‘EBA Report 2021:08, The Expert Group for Aid Studies (EBA),’* Sweden.

Mishra, Alok, Alzoubi, Yehia Ibrahim, Anwar, Memoona Javeria, and Gill, Asif Qumer (2022) ‘Attributes impacting cybersecurity policy development: An evidence from seven nations’, *Computers & Security,* 120, 102820.

Morgan, Hani. (2022) ‘Conducting a Qualitative Document Analysis,’ *The Qualitative Report*, 27(1), 64-77.

Moynihan, Harriet (2019) *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, (Chatham House: The Royal Institute of International Affairs).

Muszyński-Sulima, Wawrzyniec (2023) ‘Cold War in Space: Reconnaissance Satellites and US-Soviet Security Competition’, *European Journal of American Studies,* 18(2).

Myndigheten för samhällsskydd och beredskap (MSB) (2022) ‘Comprehensive Cyber Security Action Plan 2019–2022’, Online: (Accessed: 28 June 2024).

Naeem, Muhammad, Ozuem, Wilson, Howell, Kerry, and Ranfagni, Silvia (2023) ‘A Step-by-Step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research’, *International Journal of Qualitative Methods*, (22), pp.1-18.

Nakashima, Ellen and Harris, Shane (2018) ‘How the Russians hacked the DNC and passed its emails to WikiLeaks’, *The Washington Post*, 13 July. Online: https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html (Accessed: 26 July 2024).

Natalucci, Fabio, Qureshi, Mahvash S., and Suntheim, Felix (April 9, 2024) 'Rising Cyber Threats Pose Serious Concerns for Financial Stability', *IMF Blog*. Online: https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability (Last accessed: 30 June 2024).

NATO (2021) 'Russia's Strategy in Cyberspace'. NATO Strategic Communications Centre of Excellence.

NATO (2024) *Relations with Sweden*. Online: https://www.nato.int/cps/en/natohq/topics_52535.htm (Accessed: 20 July 2024).

NCSI (2024) 'National Cyber Security Index'. Archived data from 01.09.2023. Online: https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1 (Accessed: 20 July 2024).

New Zealand Department of the Prime Minister and Cabinet (2017) *'Defining National Security: The agencies' role in protecting New Zealand'.* Available at: https://www.dpmc.govt.nz/sites/default/files/2017-09/fact-sheet-3-defining-national-security_1.pdf (Accessed: 03 July 2024)

NTT (2024) 'NIS2 becomes the Cybersecurity Act in Sweden – this is what you need to know'. Online: https://se.security.ntt/en/nis2-becomes-the-cybersecurity-act-in-sweden-this-is-what-you-need-to-know/ (Accessed: 19 July 2024).

Nye, Joseph S. Jr. (2010) *Cyber Power* (Cambridge: Harvard Kennedy School).

Nye, Joseph S. (2011) 'Nuclear Lessons for Cyber Security?', *Strategic Studies Quarterly*, 5(4), pp. 18-38.

Observer Research Foundation (ORF) (2023) 'States' use of non-state actors in cyberspace', *Observer Research Foundation*. Online: https://www.orfonline.org/expert-speak/states-use-of-non-state-actors-in-cyberspace (Accessed:28 June 2024).

Odoh, Ejimofor Maurice (2021) 'Cyber Attack as a Tool to Influence Foreign Policy: A Comparative Study of Russia's Cyber-Attacks on Estonia and Georgia', *University of Nigeria Journal of Political Economy,* 11, pp. 18-21.

O'Dwyer, Gerard (2023) 'Sweden boosts defense spending, NATO goal in mind', *Defense News*. Online: https://www.defensenews.com/global/europe/2022/11/22/sweden-boosts-defense-spending-nato-goal-in-mind/ (Accessed: 20 July 2024).

Office of the Director of National Intelligence (ODNI). (2017). *Assessing Russian Activities and Intentions in Recent US Elections*. Online: https://www.dni.gov/files/documents/ICA_2017_01.pdf (Accessed: 19 July 2024)

Olaoye, Godwin O., (2023) 'Digital Privacy and Security in the Age of Information and Communication Technology', *Preprint*.

Ottis, Rain (2008) 'Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective'. Tallinn: Cooperative Cyber Defence Centre of Excellence.

Ottis, Rain and Lorents, Peeter (2010) ‘Cyberspace: Definition and Implications,’ *Cooperative Cyber Defence Centre of Excellence, Tallinn.* Available at: https://dumitrudumbrava.wordpress.com/wp-content/uploads/2012/01/cyberspace-definition-and-implications.pdf (Accessed: 02 July 2024)

Pascucci, CDR Peter (2017) ‘Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution’, *Minnesota Journal of International Law*, 26, pp. 257.

Pashkevich, Volha, Haftor, Darek M. and Pashkevich, Natallia (2021) ‘The information sector in Denmark and Sweden: Value, employment, wages’, *Technological Forecasting and Social Change*, (162).

Petru-Cristian, Negrea (2024) ‘Cyber Conflict and International Relations: A Comprehensive Analysis of Cyber Deterrence Strategies in Contemporary Geopolitics’. *Thesis*. Available at: https://www.researchgate.net/publication/378334428_Cyber_Conflict_and_International_Relations_A_Comprehensive_Analysis_of_Cyber_Deterrence_Strategies_in_Contemporary_Geopolitics (Accessed: 03 July 2024)

Petterson, Rune (1994) ‘Information Technology in Sweden’, *Educational Technology and Research Development*, (42:3), pp.102-108.

Polityuk, Pavel, Vukmanovic, Oleg, and Jewkes, Stephen (2017) ‘Ukraine's power outage was a cyber-attack - Ukrenergo’. *Reuters*. Available at: https://www.reuters.com/article/world/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BB/ (Accessed: 03 July 2024).

Pressel, Andria (2021) 'Sun Tzu: The Man Who Defined Chinese Warfare', *The Collector*. Available at: https://www.thecollector.com/sun-tzu-chinese-warfare/ (Accessed: 02 July 2024).

Reinking, David and Colwell, Jamie (2015) ‘A Brief History of Information Sources in the Late 20th and Early 21st Century (A Simulation)’, in Spiro, R., DeSchryver, M., Schira-Hagerman, M., Morsink, P., & Thompson, P. (eds.) *Reading at a crossroads? Disjunctures and continuities in current conceptions and practices*. New York: Routledge, pp. 3-20.

Reuters (2017) 'PM Lofven says foreign powers threatening Sweden's 2018 election', Reuters. Online: https://www.reuters.com/article/world/pm-lofven-says-foreign-powers-threatening-sweden-s-2018-election-idUSKBN1721X5/ (Accessed: 20 July 2024).

Reuters (2024) ‘*Sweden joins NATO as war in Ukraine prompts security rethink’*. Available at: https://www.reuters.com/world/sweden-set-become-natos-32nd-member-pm-visits-washington-2024-03-07/ (Accessed: 04 July 2024).

Reveron, DS, Savage, JE (2023) *'The Emergence of Cyberspace and Its Implications'*, In: Security in the Cyber Age: An Introduction to Policy and Technology,Cambridge University Press, pp. 13-34.

Richardson, John (2011) 'Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield', *Journal of Computer & Information Law*, 29(1).

Rugina, Juma Mdimu (2023) 'Economic cyber espionage: The US-China dilemma', Journal of *International Relations Studies,* 3(2), pp. 77-90.

Sanger, David E. (2020) 'Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect'. *The New York Times.* Available at: https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html (Accessed: 19 July 2024).

Schouten, Peter (24-06-2012) 'John Mearsheimer on Power as the Currency of International Relations, Disciplining US Foreign Policy, and Being an Independent Variable,' *Theory Talk #49.* Online: http://www.theory-talks.org/2012/06/theory-talk-49.html (Accessed:28 June 2024).

Schroefl, Josef (March 2020) 'Cyber power is changing the concept of war', *Hybrid CoE Strategic Analysis,* 21.

Sebenius, Alyza (05/12/2023) 'China's Hackers Are Expanding Their Strategic Objectives'. *Lawfare.* Online: https://www.lawfaremedia.org/article/china-s-hackers-are-expanding-their-strategic-objectives (Accessed: 26 July 2024).

Sharma, Amit (2023) 'Cyber Wars: A Paradigm Shift from Means to Ends', *Strategic Analysis*, 34(1), pp. 62–73.

Shephard (2022) 'Sweden steps up cyber efforts'. Online: https://www.shephardmedia.com/news/digital-battlespace/sweden-steps-up-cyber-efforts/ (Accessed: 20 July 2024).

Simons, Jon, and Lucaites, John Louis (2017) *IN/VISIBLE WAR: The Culture of War in Twenty-First-Century America*. New Brunswick, NJ: Rutgers University Press.

Singer, Peter W. (2001) 'Winning the War of Words: Information Warfare in Afghanistan', *Brookings Institution*. Available at: https://www.brookings.edu/articles/winning-the-war-of-words-information-warfare-in-afghanistan/ (Accessed: 02 July 2024).

Smeets, Max and Lin, Herbert S. (2018) 'Offensive Cyber Capabilities: To What Ends?', in Minárik, T., Jakschis, R., & Lindström, L. (eds.) *2018 10th International Conference on Cyber Conflict CyCon X: Maximising Effects*. Tallinn: NATO CCD COE Publications, pp. 55-72.

Snyder, Hannah (2019) 'Literature review as a research methodology: An overview and guidelines', *Journal of Business Research*, (104).

Štrucl, Damjan (2021) 'Comparative study on the cyber defence of NATO Member States,' *NATO Cooperative Cyber Defence Centre of Excellence.* Available at: https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf (Accessed: 02 July 2024)

Stytz, Martin R., and Sheila B. Banks. (2014) 'Toward Attaining Cyber Dominance,' *Strategic Studies* 8(1), pp. 55-87.

Svyrydenko, Denys, and Wiktor Możgin (2022) 'Hacktivism of the Anonymous Group as a Fighting Tool in the Context of Russia's War against Ukraine,' *Future Human Image,* 17, 39-46

Swedish Armed Forces (2023) 'CYBER DEFENCE'. Online: https://www.forsvarsmakten.se/en/about/organisation/cyber-defence/ (Accessed: 20 July 2024).

Swedish Armed Forces Headquarters (2024) 'Sweden and the United States deepens the partnership in cyber defense'. Online: https://www.forsvarsmakten.se/en/news/2024/04/sweden-and-the-united-states-deepens-the-partnership-in-cyber-defense/ (Accessed: 20 July 2024).

Swedish Civil Contingencies Agency (MSB) (2019) *Comprehensive Cyber Security Action Plan 2019–2022 – March 2019*. Swedish Civil Contingencies Agency (MSB).

Swedish Civil Contingencies Agency (MSB) (2020a) *Comprehensive Information and Cyber Security Action Plan for the years 2019–2022 – Report 2020* (Stockholm: Swedish Civil Contingencies Agency).

Swedish Civil Service Agency (MSB) (2020b) *Total Defence Exercise 2020*. Online: https://www.msb.se/en/training--exercises/ovningar/total-defence-exercise-2020/ (Accessed: 20 July 2024).

Swedish Government (2017) *A national cyber security strategy* (Stockholm: Government Offices of Sweden).

Techeconomy (2024) Countries with the Highest and Lowest Risk for Cyber Threats Worldwide in 2024. Online: https://techeconomy.ng/countries-with-the-highest-and-lowest-risk-for-cyber-threats-worldwide-in-2024/#:~:text=Sweden%20takes%20a%20proactive%20approach,strong%20cybersecurity%20readiness%20and%20preparedness (Accessed: 20 July 2024).

Tepe, F. Fulya (2007) 'Swedish Neutrality and Its Abandonment', *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi,* 6(11), pp. 183-201.

Tewari, Brigadier Saurabh (2019) *'International Cooperation in Fight Againstcyber-Crime'* (New Delhi: Centre for Joint Warfare Studies (Cenjows)).

The International Institute for Strategic Studies (IISS), (2023) 'CYBER CAPABILITIES AND NATIONAL POWER Volume 2'. Online: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2.pdf (Accessed: 26 July 2024).

The Local (2017) Sweden PM 'can't rule out' Russian interference in Swedish elections. Online: https://www.thelocal.se/20170109/sweden-pm-cant-rule-out-russian-interference-in-swedish-elections (Accessed: 26 July 2024).

The Swedish Defence Commission (2020) *The Swedish Defence Commission's white book on Sweden's Security Policy and the Development of the Military Defence 2021-2025*. Online: https://www.government.se/globalassets/regeringen/dokument/forsvarsdepartementet/forsvarsberedningen/slutrapport-14-maj/defence-commissions-white-book-english-summary.pdf (Accessed: 20 July 2024).

The White House (2009) 'Remarks by the President on Securing Our Nation's Cyber Infrastructure'. Online: https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (Accessed: 19 July 2024).

The White House (2023) *Cybersecurity Strategy March 2023*. Online: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (Last accessed: 03 July 2024).

Tran, Delbert (2018) 'The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack', *The Yale Journal of Law & Technology,* 20, pp. 376-441.

Tronnier, Frédéric, Pape, Sebastian, Löbner, Sascha, and Rannenberg, Kai (2022) '*A Discussion on Ethical Cybersecurity Issues in Digital Service Chains'*, in Joanna Kołodziej, Matteo Repetto, and Armend Duzha (eds.) *Cybersecurity of Digital Service Chains: Challenges, Methodologies, and Tools* (Switzerland: Springer), pp.222-256.

The International Institute for Strategic Studies (IISS), (2021) 'CYBER CAPABILITIES AND NATIONAL POWER: A Net Assessment'. Online: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf (Accessed: 28 June 2024).

U.S. Department of the Navy (2023) *Department of the Navy Cyber Strategy.* Online: https://media.defense.gov/2023/Nov/21/2003345095/-1/-1/0/DEPARTMENT%20OF%20THE%20NAVY%20CYBER%20STRATEGY.PDF (Accessed: 02 July 2024).

United Nations Office of Counter-Terrorism (UNOCT) (2022) *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices 2022 Update*. UNOCT.

Usiemure, Oghenerioborue Christopher and Gbigbidje, David Lawson (2018) 'Realist Theory of International Relations', *The International Scholar Journal of Arts*, 1(1).

van Haaster, Jelle (2016) 'Assessing Cyber Power', *8th International Conference on Cyber Conflict.*

Vivek, Ramakrishnan, Nanthagopan, Yogarajah, and Piriyatharshan, Sarmatha (2023) 'Beyond Methods: Theoretical Underpinnings of Triangulation in Qualitative and Multi-Method Studies', *SEEU Review*, 18 (2), pp.105-122.

Voo, Julia, Hemani, Irfan, Jones, Simon, DeSombre, Winnona, Cassidy, Dan, and Schwarzenbach, Anina (2020) 'Reconceptualizing Cyber Power: Cyber Power Index Primer,' *China Cyber Policy Initiative.* Online: https://www.belfercenter.org/sites/default/files/2020-04/ReconceptualizingCyber.pdf (Accessed: 02 July 2024).

Wahlbäck, Krister (1998) 'Neutrality and Morality: The Swedish Experience', *American University International Law Review*, 14(1), pp. 103-121.

Warchał, Arnold, and Piotrkowski, Kazimierz (2023) 'Information and Modern Technologies as An Asymmetric Threat to State Security. Philosophical Perspective.', *Journal of Modern Science,* 4, pp. 578-591.

Williams, John Allen, Cimbala, Stephen J., and Sarkesian, Sam C. (2022) *US National Security: Policymakers, Processes, and Politics. 6th edn.* (Boulder: Lynne Rienner).

Wong, Audrye (2022) 'The Age of Informational Statecraft'. Online: https://www.project-syndicate.org/magazine/informational-statecraft-china-russia-undermining-democracy-by-audrye-wong-2022-06 (Accessed: 19 July 2024).

Wray, Christopher (2019) 'Global Terrorism: Threats to the Homeland'. Online: https://www.fbi.gov/news/testimony/global-terrorism-threats-to-the-homeland-103019 (Accessed: 19 July 2024).

Wyrębek, Henryk (2022) 'National Security Challenges and Threats', *Wiedza Obronna*, 279(2).

Yannakogeorgos, Panayotis A. (2016) *Strategies for Resolving the Cyber Attribution Challenge* (Alabama: Air University Press).

Ylönen, Aleksi (2022) 'A Critical Appraisal of Realist International Relations Concepts in the Horn of Africa-Persian Gulf Relations: The state, power, and agency', *Centro de Estudos Internacionais*, pp. 41-69.