Lunds Universitet
Samhällsvetenskapliga Institutionen
Freds- och Konfliktvetenskap

FKVK02
VT19
Handledare: Roxanna Sjöstedt

A review of Sweden's cyber security actors through the lens of Assemblage theory

An examination of the contributions and possible friction between the actors involved in Sweden's cyber security with special consideration towards the public-private sector

Number of characters: 63515
Andrea Brodin

Abstract

Our entire society relies on technologies to function. Critical infrastructure like: water, power, transportation and communication systems amongst other things are technologies connected to the cyberspace. The cyber security is therefore to be considered a matter of national security, hence it also needs to be handle like a national security matter. Many states has come to the conclusion that public-private partnerships are the best solution in order the handle the contemporary cyber security challenges. However how these partnerships should be conducted is not as defined. Through the lens of *Assemblage theory for cyber security,* Sweden's cyber security and the actors involved with special consideration for the public-private sector, are examined with the aim of locating contribution and possible friction. It appears that there has been friction between the public and private actors at some occasions. However as it regards the national security these frictions are rarely mentioned and if they are, it is often the media that has exposed them.

Key words: Cyber security, Sweden, public-private partnerships, assemblage theory, national security, friction, assemblage

Table of Contents

1. Introduction

The contemporary society is highly dependent on technologies. It ranges from getting electricity to getting news, the ability to quickly contact one another to the ability to conduct business. Our entire society is used to be able to rely on technologies and their functions. The technology industry is ever evolving and the evolution is moving fast, however it is not without risks. There is a large range of different types of technologies and a large part is connected to the cyberspace. Everyday there are cyber attacks occurring around the world targeting different objects. These targets could be everything between an ordinary person to multinational corporations or governments. According to the Global Risks Report 2019 there were massive breaches of personal information in 2018. Where the largest was in India's government ID database, Aadhaar, where potentially all 1.1 billion registered citizens were compromised.

This raises concerns about the security. One could ask if it is a national security problem. According to the Global Risks Report 2019, cyber security issues should be considered a national security problem, partly since the potential vulnerability of critical technological infrastructure poses a risk to the nation. In the US, hackers had gained access to the control rooms of US utility companies in July 2018. Pairing of cyber attacks with critical infrastructure breakdown was the second most frequently cited risk interconnection according to the Global Risks Report 2019 (World Economic Forum 2019).

Furthermore this leads to questions regarding if the state should be the one in charge of the cyber security or could private firms handle this kind of threat. In many states there is a mixture of public-private partnerships to address the cyber security issues. The private sector even holds key position on some cyber security matters (Eichensehr 2017). At the forefront of contemporary cyber security challenges sits multinational corporations, hacktivist groups, intergovernmental organisations, and volunteers and they all provide or threaten the cyber security. In other words, all non-state or non-traditional actors. These actors have all helped to develop meaningful capabilities in the cyber-related industry and they have been able to do so perhaps thanks to the historically prominent role of private actors in this industry or thanks to the low barriers to entry (Collier 2018).

The purpose of this thesis is to examine the contributions of and possible friction between the actors involved in Sweden's cybersecurity. Hence the first step is to lay out what actors are involved and the second step will be to figure out how they interact with consideration towards power relations and the practice that embed the actors together. The main focus will be to locate if there is a friction between the actors with special consideration towards the private- and public sector. Through the lens of the Assemblage theory and with James Collier's interpretation of this theory I hope to locate the mechanism behind Sweden's cyber security, the actors that are in play and how they interact. The research question is therefore what follows:

"How do key actors in Sweden's cyber security interact and whether that constitutes friction with special consideration towards the public-private sector?"

The contemporary cyber security challenges poses a great risk towards the national security. Hence examining this field generates both theoretical and social relevance. With the method of process tracing, I aim to generate external validity and make a contribution to the scientific field of cyber security.

2. Theory

In order to produce a comprehensive picture of the contemporary cyber security and its challenges the first order of business will be to present the existing research field. Primarily the cyber security research, secondly the cyber security research with focus on public-private partnerships (referred to as PPP). Thirdly presenting assemblage theory and the background for the theory framework I have chosen.

2.1 Previous cyber security research

Before proceeding with the previous cyber security research I find it important to define the term *cyber security*. In most literature the term is used as an all-inclusive term and definitions of it may vary (Solms and Niekerk 2013). The International Telecommunications Union (ITU 2019) define cyber security as follows:

> *"Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment."*

The cyber security issue may for some seem rather new, however others may argue the contrary and simple say that it rather took decades before the general public recognized its salience. Michael Warner argues that the cyber issue was three decades old before, at least, American policy-makers and officials recognized the threat it poses and developed cyber security. The underlying reason these policy-makers and officials came to realise this was, according to Warner, four insights. These insights were that computers can spill sensitive data, that computer can be attacked and data stolen, that humans have the ability to build computer attacks into military arsenal and lastly that other humans, than themselves, also could build that and perhaps already were. Hence they developed cyber security (Warner 2012).

The threats that cyber security is supposed to handle includes attacks on critical infrastructure like: water, power, transportation and communication systems. However it is not only the attacks that poses a great risk. Some terrorist organisations use the internet, mobile phones and other information and communication technologies for recruiting, organizing and also fundraising. This "new" domain of threats lead to an arms race in cyberspace according to Ron Deibert and Rafal Rohozinski. They mean that state militaries, extremist, non-state actors, private actors who in some states control the infrastructures of cyberspace and other organisations became engaged in aggressive interventions (Deibert and Rohozinski 2010).

2.2 Public-private partnerships in the cyber security

to handle these threats alone. The private sector have become a (co-)responsible partner in handling the various threats and risks, among those the cyber security challenges (Kjægaard Christensen and Lund Petersen 2017). Moreover this shift have also resulted in growt
With regard to cyber security challenges, PPP is, according to many states, the answer. The nation-state no longer has the predominant security role. Threats and risk have undergone a change and become more elusive and unpredictable. Therefore the nation-state no longer has the same capabilities h in the research field regarding both cyber security and more precise PPP in cyber security.

All around the world states have established specialized cyber security agencies and adopted national cyber security strategies. NATO has declared the cyberspace as an official domain of warfare. A cyber attack has the potential to trigger a collective response from NATO acting under Article 5. With this cyber threat escalation the PPP have become the resort many states turns to. These PPP are supposed to voluntarily share knowledge on national security and take responsibility for ensuring an effective management of cyber threats. However there is no clear definition of what kind of knowledge the different partners should share with each other. Additionally there is a discussion about what even counts as cyber security knowledge. This knowledge problem is situated at the heart of the dilemma between private and public, the economic interest versus the security interest (Kjægaard Christensen and Lund Petersen 2017). Thus the question arises, is PPP a market-driven approach to cyber- and, ergo, national security? Madeline Carr asserts that there is no common ground for the security interest between private and public actors. Furthermore there is a reluctance of politicians to introduce tougher cyber security measures by law as well as the private sector expresses a reluctance to accepting responsibility for national security. Hence PPP is left without clear lines of responsibility or accountability. It is an extremely delicate matter for the government to pass on its core task and responsibility of generating security for citizens on to the private sector (Carr 2016).

Nevertheless the PPP is still considered a cornerstone in many states' cyber security, especially those where critical infrastructure systems in areas such as utilities, finance and transport have been privatized (Carr 2016). Knowledge-sharing between those privatized critical infrastructure companies and authorities is highlighted as a means to mitigate the shared risk in cyber security. It is seen as a way of governing the uncertainty of cyber security risks. Although, as mentioned above, there is no agreement over what knowledge to be shared. They might agree that the cyber security risks are there to be shared, however they have different notions of what counts as the knowledge that will help mitigate the risks (Kjægaard Christensen and Lund Petersen 2017).

There is, both within the relevant policy documents and within the cyber security discourse generally, the fact that the PPP are often referred to as a single entity, ignoring its complexity. Therefore one of the contributions this thesis seeks to make is unpacking the term and showing the complexity and diversity. Also, as Carr points out, many cyber security aspects are linked to national *interest*, although critical infrastructure protection is unequivocally and intrinsically linked to national *security* (Carr 2016). Therefore it is highly relevant to conduct this type of research within peace and conflict studies. It is to be considered a security problem.

2.3 Assemblage theory

Assemblage theory is meant to apply to a large variety of whole constructed from heterogeneous parts. Meaning it is meant to be a very broad theory that could be used to explain many different objectives that in turn, are or could be constructed by a variety of actors. Assemblage as a theory made its first appearance in Deleuze's work (much of it in partnership with Félix Guattari) *A Thousand Plateaus* (1987). What Deleuze presented in his work was, however, hardly a fully-fledged theory. Drawing from his other work one could see that his concepts used to specify the characteristics of "assemblage theory" in *A Thousand Plateaus* are most connected and elaborated with his concepts in his other work. By puzzling his different work together, at least the fundamentals of a theory was presented (DeLanda 2019). Much of what the assemblage theory is build upon is a number of developments in scientific thought that matured in the twentieth-century. The development of the non-linear sciences with the concepts of open systems, complexity, emergence and non-linear dynamics. By using the tools that had been developed to describe such phenomena and drawing upon developments in mathematics and biology he developed the foundation of assemblage. *"A way of conceptualizing the various entities of the natural and social world as assemblages of heterogeneous components that are always transient and open, and in process, never solidifying into a closed totality or system"* (Acuto and Curtis 2014). In other words, Assemblage theory is a theory that desire to form some sort of concept of both the natural and social world. This as the both of these worlds are built upon different actors and components that are impermanent, ever changing and ever evolving.

Amongst many others, Manuel DeLanda has made his own interpretation of Deleuze's theory into a more comprehensive theory of assemblage. Some Deleuzians has been against DeLandas work, however he does make clear that it is his own definitions of the theory (DeLanda 2019). His work has nevertheless provided a clarification of the theory. He brings up the rapid development of computer technology as an important methodological tool for scientist to use while uncovering the dynamics of assemblages. Through the use of computer technology the scientist can easier find a substantial amount of data, as needed when conducting a study with the use of Assemblage theory. Furthermore other thinkers has also contributed to the field. Saskia Sassen used the concept of assemblage as a tool to untangle the dynamics of how the modern world emerged from social structures from the premodern world. Much like Sassen, Aiwa Ong and Stephen Collier has explored assemblage thinking as a way of looking at the global assemblages and the governance logics of the diversity. These thinkers, Sassen, Ong, Collier and also Deleuze have all been invoked in contemporary international relations writing. Their approaches are in contrast of many of the theories, concepts and tools that are currently the main approach in understanding social change and the reconfiguration of institutions.

Naturally assemblage thinking has been given some critic. Many mean that there is an inherent analytical danger. This because it can easily fall prey of a self-reinforcing process of endless deconstruction. Hence it is a method of unpacking categories, it may eventually reach the question of where to stop assembling and disassembling. For example, assemblages like "the state" might unveil other smaller totalities and they might in turn hold internal realities that needs to be disentangled and so on (Acuto and Curtis 2014). Therefore when conducting a study using the assemblage theory one must have clear definitions of what to examine, what time frame and how. It is also very important to thoroughly explain each step in order to make it clear why it was made. By doing this one could demonstrate and discuss that the assembling or disassembling, in the study, is not a process of endless deconstruction, but rather necessarily for the detailed analysis.

2.4 'Assemblage theory for cyber security'

In the following part of the studie I will define and operationalize the theory framework. As I have chosen to use Colliers interpretation of the assemblage theory the following definitions will be accordingly to his interpretation. He means that instead of the earlier frameworks of assemblage it is more appropriate with a five-shift process of assemblage formation in a cyber security context. However in doing this the objective is not to provide a comprehensive history of events. Instead the objective is to show how the various actors have developed and intertwined together in the context of cyber security. He therefore reserves himself from critic by acknowledging that his five shifts are overlapping and not necessarily perfectly linear. Furthermore with the word 'cyber' being a broad catch-all term that compromises a number of separate processes (including encryption disputes, disinformation campaigns, and internet governance), not all issues within the concept has developed in the same way. This is why it is important to keep in mind that the following five shifts represents a broad generalisation and not a precise account of specific cyber security issues (Collier 2018).

One: Development of Underpinning Technologies

According to the theoretical framework, one can not stress enough the importance of understanding the background for the contemporary cyber security. Hence the first step in the assemblage theory framework is to collect knowledge of the history of the cyber security. Furthermore since computers and computer networks is the very foundation of the cyber security, the development of these two is what can be marked as a starting point for this framework. When applying to a case the timeframe will naturally differ, depending on when the case in matter comprehended and/or developed this type of technology. Focus is naturally on the actors involved.

When Collier describes this first shift, he does not apply it to a single state or case, he rather describes the development worldwide. Hence he begins with the first programmable computer that was built between 1936 and 1938 by German Konrad Zuse. The foundation for theories about computing and computers was the Turing Machine and it was proposed in 1936 by Alan Turing. In 1946 the first electronic computer was used for general purpose, the Electronic Numerical Integrator, invented by John presper Eckert and John Mauchly. Hence it is slightly problematic to declare when the first computer was built given the range of classification. However the "when" is not what is important, rather the "who", the actors involved.

Computer networks has a more coherent history as the first paper on switching theory was published in 1961. The ARPANET were being developed by the late 1960s and by 1969 the first host computer, a Network measurement Center at UCLA, was connected. Hence the creation of both computers and computer networks was an assemblage of different actors. The academia was at the forefront, however both states and private actors played vital roles (Collier 2018).

Two: Development of the Private Sector

The second shift is regarding the development of the private actors. In this shift it is important to only focus on the development of the private actors. Focus on what role they have played and how they have developed. When Collier applies this shift in his theory framework it, along with the third shift, lays the foundation for the fourth and the fifth shift.

Collier continues in a chronological order after the first shift with describing the development of the network. This becomes quite natural as when the ARPANET was decommissioned in 1990 it opened up opportunities for other private sector firms to invest in this type of research and development. Hence what followed was several US computer manufacturers, software vendors and internet service providers began to develop capabilities at a global level. During this firms such as Apple, IBM and Microsoft grew swiftly. Much thanks to these private firms the cyberspace grew exponentially and it became an integral part of our contemporary society. However it also grew into an increasingly important issue. In the contemporary cyber security challenges we often see private actors at the forefront and this naturally has to do with the history of private sector driven growth of networks.

With this growth many of these private actors has also taken on a political role. Examples of this could be Google that for example has protected the identities of protestors or their measures they have developed to steer away potential ISIS recruits from the terrorist cell. Even if some private actors choose to take on this political role some private actors do not have a choice in the matter. Furthermore even if some private actors have become political actors in a cyber security context, it does not mean that they are necessarily competent in such a capacity. However many political, ethical and security challenges are lunged upon these actors. For example, social media platforms have failed to deal with some disinformation campaigns and have been given critic for this (Collier 2018).

Three: State Realisation

As mentioned in the second shift, by describing the states development in regard to cyber security, the foundation for shift four and five is layed. Therefore in this shift the focus is on the state actor and what role it have played in regard to cyber security.

Collier means that states have on the whole responded slowly to the emerging cyber security challenges (with certain military and intelligence agencies an exception). As the society became more and more dependent on computers and networks, states gradually realised the importance of developing their own cyber security capabilities and have eventually started to invest significantly in the matter. Naturally dependent on the government objectives have lead to some divergence in the cyber security development (Collier 2018).

Four: Emerging Hybridity and Contestation

The fourth shift in Colliers assemblage framework is addressing the assemblage of actors that computer and networks have comprised. These actors includes private sector, governments, academia and advocacy groups and with time this has only increased and become more complex. Out of this, increasingly hybrid structures has emerged. With hybrid structures Collier means *"[..]assemblages that embed a range of actors and transcend traditional global-local and public-private distinctions"*(Collier 2018). He exemplifies this with information sharing partnerships that exist with active participation from both public and private sectors, which could be government and corporations entities. It could also be hacker groups working together with government actors to eliminate the cyber security threats or develop measures to handle these threats. At times these hacker groups operate independently, representing the state's interest but without explicit instructions from governmental actors however often these type of activities are state-directed. These type of relationships is presented as state-proxy relationships that imply a certain binary relationship between two actors. This arrangement that is neither public or private security is, according to Collier, captured more coherently through an assemblage lens.

This type of security assemblages are often marked with competition, struggle for power and influence. The tension within these arrangement has increased and is not always a stable structure. Much of the tension is about visions of what should be public and private. With the state increasing their cyber security capabilities they have also become more assertive and willing to challenge established private sector norms which has fueled this tension (Collier 2018).

Five: Generativity

Generativity points to the emergence of new actors and processes. This is different from the previous shift as this focuses on the *new* actors and the previous focuses on pre-existing actors that are comprised into hybrid structures. The term generativity was espoused by Jonathan Zittrain who refers to it as the way that *"[..] malleable nature of digital technologies (such as the internet) allows them to serve a variety of purposes, potentially providing a platform for innovation that may not have even been foreseen by their creators"*(Zittrain, 2006). The majority of computers are able to be used for a range of processes that it was not initially designed for. Collier uses the example of Twitter, as to point out that computers built before the launch of Twitter in 2006 were still able to run the service provided that they had internet connection and internet browser.

However the generativity is also the emergence of new actors and processes. To describe this Collier use the example of the WannaCry ransomware worm outbreak. What lead up to this was firstly the development of a number of exploit tools to be used for intelligence gathering and offensive cyber operations by the US National Security Agency (NSA). Further on the Shadow brokers (identities remain unidentified) leaked this and then it was used as a part on the WannaCry ransomware that was deployed by North Korea (Goodin 2017, Grossman 2017, Volz 2017). In this there are a number of different processes that have become embedded. Another example is the response to malware, where hardware and software vendors tried to protect their own services and products and it did not take long for the anti-virus industry to form (McAleavey, 2011). This type of knock-on effect have generated many new actors and processes and probably will continue to do so. Examples of this could be the emerge of different actors that sell malware tools such as white-hat hackers, bug bounties and crypto-markets. This online malware market will in turn lead to new cybercrime and government police units. There are many of this type of examples with cyber security where the implications of an emerging technology is highly uncertain (Collier 2018).

2.5 Theoretical assumption

As Collier points out in the theoretical framework, cyber security is a complex term that involves many actors and processes. With this in mind, my theoretical assumption is that within Sweden's cyber security there is most likely some friction between the public and private actors. However to locate this friction might prove harder. As mentioned in the previous research of PPP I believe there might be some uncertainty regarding the information sharing process, of what information to be shared. Furthermore there might also be some uncertainty regarding who is responsible for the security. These issues are some that I believe might grow into a friction between the actors. I believe that some friction might be a natural element in all types of relations or partnerships however I do also believe that in regard of this being a national security matter, it is important to locate and shed light on these possible frictions in order for them to be handled. One must keep in mind that cyber threats are threats to the national security. This as a potential cyber attack can wipe out critical infrastructure like: water, power, transportation and communication systems amongst other things connected to the cyberspace. The cyber security is a matter of national security, therefore it also needs to be handle like a national security matter.

3. Method

The following section is regarding the methodological aspects of the thesis. I will describe the design, what kind of study this is, what I based my case selection on and what method I will use for this study. Furthemore I will also explain what material I will use, the limitations and the chosen timeframe.

3.1 Design, case study and case selection

The design of this thesis is a qualitative descriptive study. As my aim with this thesis is to describe and interpret the single case study of the contributions of and possible frictions between the actors involved in Sweden's cyber security, this will be an idiographic case study. An idiographic case study is a study which aim is to *"[..] describe, explain, interpret and/or understand a single case as an end in itself rather than as a vehicle for developing broader theoretical generalizations"*(Levy 2008). Since the examination object is the contributions of and possible frictions between the actors involved in Sweden's cyber security over a set time period, the study can also be typed a historical one. Most of the historical studies falls under the category of idiographic studies. Moreover it is a theoretical guided study as it is structured by the explicit theory framework of Collier's interpretation of assemblage theory. The aim is not to generalize beyond the data rather, as mentioned above, describe and interpret this single historical episode. Some mean that this type of study should only be conducted by historians and not by social scientists, as the aim is not to generalize beyond the data. However important to keep in mind is that even though the aim is not to generalize the data the theory can still be generalizable. Through the explicit and structured use of theory to explain the one particular case, as will be for this particular study, the results are often excellent explanations and understandings of key aspects, many times better than the ones made by historians, argues Jack S. Levy (2008).

I based my case selection on finding a relevant case for both the application of the Assemblage theory framework and on making a contribution to a relatively non researched scientific field. Furthermore as the chosen theory framework is relatively new and this exact type of case study never has been done, to the extent of which I know, any chosen case would to some extent contribute to the field. Hence the choices of cases was not particularly narrow. However I wanted a case that would have high theoretical and social relevance. Therefore I considered

Sweden to be a relevant case for this study as I will argue that it contribute to both the theoretical and social criterias. This, as Sweden is a high technology country. 98% of the population in Sweden had in 2018 access to internet from home (Statista 2019). Not only is the information and communication technology important to inhabitants of Sweden, it also play an essential role for the government. The Swedish government have tried to digitalise its operations as much as possible. Through the use of eHealth, eGovernment and more, they aim to bring their citizens closer by enabling access to public or state services via the Internet. Naturally this has its risk which the Swedish government is well aware of. They have developed a concept of total defence when tackling the cyber security challenges. This concept insinuate partly that Sweden analyses other informationally and technology developed states, how they have handle their cyber security challenges. Beyond observing other state actors, Sweden also engage the private sector and individuals to work in a partnership with the government in order to confront the threats in cyberspace (Svete 2012). Furthermore Sweden is a member of the EU which in turn has regulations regarding the cyber security for its member states. This also makes Sweden, or any other EU country, interesting for the assemblage theory framework since the EU is a form of assemblage in itself.

Another criteria was the amount of data that I could comprehend. Since the very essence of Assemblage theory is in details, each and every one of the different shifts require a substantial amount of data to be complete and concluded. Therefore the data availability is extremely important to take into account when choosing case for this precise type of study.

Moreover another factor I considered was the previous research done in the field. I wanted a case that was relatively unexplored. Unexplored in a sense that it was new in either the Assemblage field or the PPP cyber security field. All of these criterias lead up to my case selection of Sweden.

3.2 Process tracing

The method I have chosen for my study is process tracing, developed by Andrew Bennett and Alexander L. George. Process tracing can be referred to as tracing a sequence of events that brought them about. Many have pointed out the similarities to historical explanations. Some of the arguments of the differences are stated above in the design, case study and case selection section. Process tracing is different from a historical narrative as it converts a purely historical account into an analytical explanation couched in theoretical variables that have been identified in the research design. This has been given some critic by historians. They mean that by converting a rich historical explanation into an analytical explanation, some of the uniqueness as well as some important characteristics may be loss. This may be the case sometimes, some information may be loss and as an investigator one should be aware of this and consider the implications of this towards the study. However it may still be important and relevant to convert historical explanations into analytical theoretical ones for the purpose of theory development. Theory-based process-tracing is employed in studies that attempt to provide explanations for specific cases and also to test and refine available theories and hypotheses. This thesis will be theory-based in an attempt to test the theory on the case of Sweden's cyber security.

The general method of process tracing presents two different approaches, a distinction which is very important to maintain. Those two are "process verification" and "process induction". The first term involves testing previously designated theories and observing whether the processes among variables match those predicted by the theories. This is what is known as a deductive approach and that is the approach that will be used in this thesis (George and Bennett 2005).

3.3 Material, limitation and timeline

The material used for this study consists of both primary and secondary material. It ranges from academic literature, documents, historical accounts to news articles, blogs and other secondary material sources. Naturally these sources will be viewed through a critical and sceptical lens. However using a secondary source might not always be the prefered option, that does nevertheless not mean that it is a source without relevance.

As mentioned above, when conducting a theoretical driven study and not a historical explanation, some information may be loss due to the theoretical approach and not the historical approach. Some details that matter for the history might not matter for the theoretical analysis and therefore some details might be excluded from this thesis. As the main focus is the cyber security and the actors involved, this is where the focus will lay. Furthermore another limitation will be the public-private partnership approach I have chosen for this thesis. Therefore there will be a greater focus and detailed analysis on mainly shift four, but also, two and three. The first shift will lay ground for the following shifts. The fifth shift, generativity, focuses on new actors and the process of how they have emerged. This is naturally very important for the cyber security as it presents new risks and threats, but also new solutions. However it is not what I aim to study, therefore, there will not be as much focus on this shift.

The timeline is from December 1948 until February 2019. The reason for the beginning is because of when the computer technology in Sweden was developed. As the cyber security has no “end date”, I have to chose one myself for this thesis. In order to comprehend as much present information as possible I wanted to include all of 2018. Since I found an illustrative example for the thesis I chose to include this example as well and then put the end date to my timeline. Therefore the timeline ends in February 2019 when articles of the example was published.

4. Assemblage theory: an analysis of Sweden’s cyber security

In the following part of this thesis the data along with an analysis according to the chosen framework, Assemblage theory, will be presented. In the same manner as Collier presented his framework, this part will also be divided into six shifts. In each shift there will be a presentation of the data and also an analysis of this data.

4.1 One: Development of Underpinning Technologies

The first step is to present the development of the underpinning technologies. As this is a case study of Sweden, it will focus on the technology and information technology (IT) development in Sweden.

In December 1948 the commission on mathematical-machines was formed, this on the initiative of the government. They were supposed to evaluate how many computers Sweden would need and who would use it. The commission developed what is called Sweden’s first computer, a Binary Arithmetic Relay Calculator (Binär Aritmetisk Relä Kalkylator), BARK. BARK was finished in February 1950. The second, more known, swedish computer was the BESK, Binary Electronic Sequence Calculator (Binär Elektronisk Sekvenskalkylator). The Besk was finished in 1953 in Stockholm and was during a couple of weeks the world's fastest computer. It was used for weather data for SMHI, statistic for state utility, profiling the wings for Saab 32 Lansen and simulations for the nuclear industry. Moreover it was also used for some minor parts in the swedish nuclear weapon program. Although the main user was national defence radio facility. However this system was not without it faults. Apparently one could with an regular car radio tap the pipes and listen in to the radio. Even with its errors the Besk was very successful. It was runned for 12 years and made 40 million sek for the government, this from fees from the customers. In 1963 the commission was dismantled and 3 years later the Besk as well. During this, the developers of the computer, had been declined by the state to build a new machine. Hence many of the engineers had moved over to the commercial market (Dahlin 2014).

As mentioned earlier, the world's first network was the ARPANET in 1969 and in 1971 the first electronic mail was sent. The word internet was first mentioned when the ARPANET went viral in 1973. In 1978, Sweden, Jacob Palme and Torgny Tholerus develope the KOM-system which can be compared to the ARPANET (Löwenfeldt 2019). Their idea was to design computer systems to aid ordinary people. Instead of the state using computers to control citizens, they wanted the citizens to control the use of computers (Palme 2015). However this was commissioned by the Swedish Defence Research Institute (FOA). Their idea in turn, was that the KOM-system was supposed to help facilitate the internal communication, when one part of the office moves to another part of the country, a new conferencing system. Important to mention as well is that Tholerus at the time was an employee at Uppsala University, so the development of the KOM-system was a grant from FOA to Uppsala University (Palme 2015). Although the KOM rapidly develops to something else (Internetmuseum 2019a). The KOM is a BBS, a bulletin board system, which in simple terms is a community where one could discuss with others, send internal messages and download files (Internetmuseum 2019b). As this is the function of it, it developed into a social hotspot for those with a computer interest, to conduct discussions (Internetmuseum 2019a). From 1982 the KOM-system was connected to the ARPANET, which made it possible for the users of the KOM-system to send emails (Löwenfeldt 2019). However it was first in 1983 that the first swedish person receives an email. His name was Björn Eriksen and he would play an important role in Sweden's internet history as he later on had the patent on the .se domain. Will return to this later.

As the internet evolved it was at first only the Universities that had the pleasure of this evolution. Through what is called "Sunet", all of Sweden's universities were linked through one network, hence they were able to communicate and send files and documents to one another. Later on all the Nordic Universities were linked through the "Nordunet" which, in 1988, was linked with Princeton in New York. Meaning that the students and scientists had access to an international internet. The common people however, did not have access to this network and had to settle with the BBS system at the time (Löwenfeldt 2019).

Just as Collier described in his framework, the technology and IT development in Sweden was an assemblage of a variety of actors. Both public and private actors worked together or alongside each other in order to make the technology possible in Sweden. However what is very clear is that the academia was at the forefront of it all, even though both public and private actors played vital roles. Although what is very important to point out is that the government of Sweden was very present during both the development of the computers and the computer networks. However even though they were present, they did not seem to realise the risks as there were never any mention of the security aspects.

4.2 Two: Development of the Private Sector

As the world wide web breaks through in 1989 it is a non governmental concern that embraces this development and becomes Sweden’s first internet service provider (ISP). The corporation Televerket, which was state-owned, had the opportunity to be first with this, however they preferred the technique they already had and therefore said no to the opportunity. Hence the private company Swipnet grasped the chance and introduced the www, world wide web, in Sweden (Löwengrip 2019). As Sunet and Nordunet was not for commercial use, there was a great need and desire of an internet provider for commercial use such as the Swipnet became (Internetmuseum 2019c). In 1994 a young boy named Ragnar Lönn launches the ISP Algonet. This differed from Swipnet as it focused on individuals rather than enterprises. They anticipated that they would have around 400 users within a year from the release date, however in six months they had 1500 users and after that the number escalated. This escalation was much thanks to the media that was writing heavily about the network and since there was only one ISP for individuals, everyone that wanted to try it had to use the Algonet (Lönn and Schedin 2016).

In 1995 the internet speed increased extensively from 6 Mbit/s to 34 Mbit/s as a new cable was drawn over the Atlantic. The following years was an explosion of new websites on the web. 1996 the christmas present of the year was a internet subscription. Social networks began to establish, for example the website Lunarstorm, which was one of the world's first social network and also became a huge success in Sweden.

Björn Eriksen, whom is mentioned above, had up til 1997 been running the registration of all .se domains in Sweden by himself. However it was only companies and organisations that could have their own .se domain name. This responsibility was, however, in 1997 shifted onto the foundation for internet infrastructure. This after an enquiry was conducted on the subject.

The interest in the internet was at the time growing in many aspects, not the least in investment. Everyone wanted a part of the future technology, which one could see clearly on the stock market. Framfab, Icon Medialab and Spray, all IT-corporations, invested in the growth and process of the technologies. The CEO of Framfab has even been referred to as “Broadband-Jesus”, this as he was at the forefront of advocating for the spread of the broadband across the country. In 1999 the Broadband company (Bredbandsbolaget), launched and the very same day the housing society HSB announced that 350 000 properties would be connected with broadband (Löwengrip 2019).

During this development the private sector definitely grew and became the predominant actor within IT-industry. Notebly the government ceased to hold on to their previous position in the IT-industry. Therefore the private actors filled the gap and grasped their chance and gained ground in the industry. Perhaps thanks to this turn in the development the private actors still today have a prominent role in the cyber security. Moreover much thanks to the private actors the IT-industry were able to have the development it had. Also, private actors made it possible for the rest of society to take part of the technology, which in turn also provided the industry to continue to develop into what it is today. However the risks and threats of the development neither seems to have been a prominent issue during this early stage of the IT-development.

4.3 Three: State realisation

The third step in Collier's assemblage theory framework is what he calls *state realisation*. By this he means that the state as an actors seems to have been slow on reacting to both the speed of the development in IT and also the threats and risk that goes hand in hand with this development.

In 1994 the government of Sweden spends a million sek on the creation of the KK-fondation with the incentive of promoting technology in the school system, among other things. The IT-kommission forms and promotes a variety of digital campaigns and the elections results sends out through email. Hence many of the Swedish newspapers comprehends their own websites. The prime minister of Sweden, Carl Bildt, emails the president of the United States, Bill Clinton, which makes them the first head of states to communicate through email. A couple of years later, 1998, the Swedish government decides to give every individual a discount when they buy a personal computer (pc) for their home and this results in what can be called a revolution for the pc-sale. Also this results in the fact that a lot of the swedish citizens have their very first own computer, of course with internet connection as well (Löwenfeldt 2019).

Swedish government formulated in 2005 a new draft act entitled *"Collaboration in the Event of Crises - For a more secure Society, representing an amendment to the previous draft act"*. This act stated that the National Information Strategy should incorporate the capability of handling interferences in the IT systems important to society. A year later they authorized The National Post and Telecom Agency to develop a strategy to improve the cyber security. This strategy was in 2009 improved and renamed as the Action plan for internet security.

In 2008 the government authorised the Swedish Civil Contingencies Agency (MSB) to prepare an action plan for information security. The MSB recognised many defects in the ICT related documents in Sweden. One of them was the fact that Sweden lacked a single governmental body, an national security agency within the cyber security domain, that the actors within the sphere would acknowledge. Instead there where a number of institutions operating in the sphere (Svete 2012).

The Protective Security Act was implemented in 1996 and had remained the same in 20 years, hence the need for a reform in this matter, one could argue, was considerably. This since the swedish society had during these 20 years been digitized. Furthermore many of the critical infrastructures has been privatized. Meaning that these private corporations would be responsible for the security and the sensitive information regarding these critical infrastructures. Therefore the government realised the need for some modernization regarding the security implementations and the law. The new proposed act covered many areas of security amongst them higher demands on the IT systems that matters for the national security. The old legislation did not make clear definitions which actors should be included. Therefore the new legislation proposed clear definitions regarding this matter. Hence all actors that conduct a business or corporation regarding the national security, no matter public or private, would be included in the new act. Moreover the requirements of the businesses had to be more defined. Therefore executors of these businesses needs to do an security analysis of the business and adapt those security changes that are required. The swedish government adopted this new Protective Security Act and proposed it to begin in 2019 (Abu Eid 2017, Regeringskansliet 2019).

The government of Sweden accepted their first cyber security strategy in 2017. A strategy that, according to many, was long overdue. This strategy has six priorities to promote Sweden's security and IT policy objectives. The first priority is securing a systematic and comprehensive approach in cyber security efforts. This since the government of Sweden conclude that cyber security concerns the whole of society, hence everyone needs to take responsibility. Meaning that they want to enhance the collaboration and cyber security information sharing and also improve the conditions for pursuing systematic cyber security efforts in a more integrated and coordinated manner. The second priority is enhancing network, product and system security. The government conclude that today's society is dependent on electronic communication. The access to secure data encryption systems for IT and communications solutions must meet society's needs. Furthermore the security for industrial information and control systems that control and monitor for example the distribution of electricity and supply of drinking water, must be enhanced. The third priority is enhancing the capability to prevent, detect and manage cyberattacks and other IT incidents. With this priority the government mean to conduct through increased collaboration and planning. Also through the use of adequate technical resources that will help mitigate the consequences of cyberattacks and other IT incidents. Furthermore for the activities of highest importance to the national security and systems vital to total defence, the government want an advanced cyber defence. The fourth priority is increasing the possibility of prevention and combating cybercrime. Through adapted legislation, well-developed expertise and organisational structures and enhanced international cooperation the government hope to prevent and combat cybercrimes. The government underlines the importance of more stakeholders, beyond law enforcement authorities, to actively take part in these efforts. The fifth priority is increasing knowledge and promoting expertise. This priority they aim to meet through higher education, research and development and regular training activities. The last priority is enhancing international cooperation. By this the government mean that handling and tackling the cyber security challenges requires international cooperation which is based in "[..] *international law and the objective of a global, accessible, open and robust internet characterised by freedom and respect for human rights"*(Regeringskansliet 2017a). The follow-up of the strategy will be conducted through ensurement of the achievement of the objectives by relevant government agencies. Since the technology development and the risks that follows are evolving at a rapid pace the strategy must also be able to meet this. Therefore it needs to be flexible. The government says that they *"[..]will prioritise the implementation of the strategy and closely monitor developments in the area"* (Regeringskansliet 2017a).

What can be said about all the six priorities is that they all include actors beyond the public sector. Meaning that the government of Sweden both wants and feel the need to share the security responsibility regarding the cyber security for national security. What can also be concluded is that the government of Sweden did not have a single governmental body for the cyber security until the strategy was implemented. This strategy, as will become clear in the fourth shift, was a consequence of the EU:s implementation of their legislative towards the cyber security. However the Swedish government have risen to the task and have realised that cyber security is a question regarding national security. They have also come to the conclusion of collaboration with other actors beyond the state to handle the challenges. In accordance with the framework, the state of Sweden reacting reactively instead of proactively. The consequences of reacting reactivity towards an issue is sometimes overacting. However the government seems to have concluded that there was a great need of a strategy and also that they needed the right competence for it which mean that they need to uncover this competence and they need to collaborate with it.

4.4 Four: Emerging Hybridity and Contestation

The fourth shift in the framework focuses on addressing the assemblage of actors that computer and networks have comprised. These assemblages includes actors like governments, private actors, academia and advocacy groups. Out of this hybrid structures has emerged. A public-private partnership is an example of a hybrid structure.

Swedish cyber security is full of these hybrid structures or assemblages. Through a review of the cyber history in Sweden, these hybrid structures might not come as a surprise. As mentioned, the government of Sweden has in its cyber security strategy put a lot of focus in these types of assemblages, collaborations or partnerships. In this strategy the government explicitly writes that in order to protect themselves, the responsibility has to be shared by all of society, including the government, county councils, authorities, companies and organisations in Sweden. They conclude that there is a need for clarity in terms of *who* is responsible for the cyber security efforts, both within organisations and in society as a whole. Furthermore they continue on writing that the cyber security is to be a natural and integral part of all work at all levels in society and not only within organisation and the different sectors of society, but also between them (Regeringskansliet 2017b). Where the *between* word is, according to the theory framework, of importance since that can be considered a key word for these assemblages or hybrid structures. Not only shall actors work alongside each other, they should also work hand-in-hand, together.

An example of an assemblage but also a contestation is the Swedish Transport Agency IT-scandal. The agency had contracted a foreign company to handle their IT-systems which lead to classified information, from the Swedish Transport Agency, being available for non classified personnel in this foreign country. The classified information that was leaked posed a threat for the national security. The consequences of this event was that three ministers in the swedish government faced the possibility of motions of no-confidence. Therefore the swedish prime minister chose to reconstruct the government and two cabinet ministers had to leave because of their involvement in the scandal (Ohlin 2018). Obviously there was a contestation or friction as the personnel that gained access to the information did not have the clearance. However the real issue might not have been that this personnel gain access to the information, maybe the real issue was that the responsibility of this information was placed on an actor that had no obligation of being responsible for this kind of information. Perhaps there were not any friction between the agency and the foreign contractor but there was friction between the government and the

Swedish Transport agency as someone had to take responsibility for the scandal and no one wanted to claim this responsibility.

Another example is the recent disclosure the website *Computer Sweden* made of the 2,7 million recorded calls, that were completely exposed on the internet, from the medical-guide 1177. Apparently these recorded calls were completely exposed audio files on an unprotected web server. Anyone could download and listen to these files that had been recorded since 2013. The material on the files was definitely sensitive information of the individuals calling as they stated personal identification number, symptoms, diseases and medication. The actors involved in this was the 1177, which is a website and call centre that provides information, counseling and services within health and medical care. The website is operated by Inera AB which is owned by the county council, the district and almost every local authority in Sweden. In other words it is within the public sector. They had contracted the medical entrepreneur Medhelp that in turn had contracted the sub-supplier Medicall that were the ones receiving the calls. Medicall, in turn, uses the call center-system Biz 2.0 that is operated by the swedish company Voice Integrate Nordic AB. Apparently no one of these involved actors realised the issue until they were exposed by Computer Sweden. Not only is it a scandal, it is also against the law as these audio files should be treated according the patient data law and personal records according the General Data Protection Regulation (GDPR) (Dobos 2019, Johansson and Thornéus 2019). Not only is it arguably clear that there is friction between these actors, public and private, there is also a security issue regarding who to claim responsible. As these actors claim, none of them realised that there was an issue until they were exposed. However does this mean that none of them can be held responsible? Can an organisation, cooperation that handles this kind of sensitive information really claim that they were unaware of this issue. Maybe even more importantly, if they really were unaware does this not pose as a larger security concern than the issue first presented. The new Protective Security Act states that "executors of these businesses (that concerns the national security) needs to do an security analysis of the business and adapt those security changes that are required. Perhaps this legislation was not defined enough for the intended businesses to realise what kind of security analysis they were required to do.

Another assemblage Sweden is a part of is the EU that has established their own legislative for the cyber security challenges. The Directive on Security of Network and Information systems, more known as the NIS-directive, is the first piece in the legislation which provides legal measures to handle the cyber security. This was adopted in 2016 however member states had until may 2018 to transpose the Directive into their national laws and identify operators of essential services by november 2018. The legal measures the directive provides is by ensuring that their member states are prepared by requiring them to be appropriately equipped. This the member states can do via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority. Another legal measure is cooperation among the Member

States by setting up a cooperation group. This group would also have a CSIRT network in order to promote a prompt and successful operational partnership on the specific cyber security issues and moreover share information about the risks. Furthermore the critical infrastructures that are operated by private companies have to take appropriate security measures and notify incidents to the relevant national authority (European Commission 2018).

To conclude, the EU directive which in itself is a form of assemblage, proposes new legal measures that provoke more assemblages, cooperation, information sharing, for the public sector to work hand-in-hand, together with the private sector. However how these assemblages or partnerships work in practice is another question. Even if the EU provides legal measures it is quite difficult to clarify what information to be shared. The perception of what information necessarily for the national security can differ between actors. Hence there might emerge friction between the actors.

4.5 Five: Generativity

Generativity points to the emergence of new actors and processes. Actors and processes that has emerged because of the technology development and that may not have been foreseen by its creators. This shift focuses a lot on new situations and processes that has emerged because of new developments within the technology. Therefore this shift, I argue, is not as relevant to this thesis as it points to another type of process that does not include clear public-private partnerships as the other shifts does. As this thesis aim to examine if there is a friction between the key actors involved in Sweden’s cyber security with special consideration towards the public-private sector, this shift is not as relevant for this thesis. As argued in the method, when conducting a theory-guided study sometimes some information may be excluded as it may not have any relevance for the theoretical analysis. Therefore this shift will unfortunately be excluded from this thesis. Future research might include this shift especially if they aim to examine other aspects of the cyber security than the possibility of friction between public-private actors.

5. Conclusion

"How do key actors in Sweden's cyber security interact and whether that constitutes friction with special consideration towards the public-private sector?"

Sweden's cyber security is very complexed with many involved actors. From the first shift one could tell that Sweden and swedish actors early on played a vital role in the technology development. However the risks and security aspects does not appear to have had a prominent part of the development. Perhaps individual actors did realise the risks but security actors such as the government or other public actors, that did use the computers or the network, does not seem to have taken the risks into account. As the development was mainly driven by private actors they may not have felt the same responsibility towards the national security aspects as perhaps public actors would. Perhaps that is one of the reasons why it took a long time for cyber security strategy to develop and to form legislation regarding the matter. Once the state did realise the issue at hand and develop the measures to handle this they also realised, it seems, that they needed help in handling these issues. Therefore the strategies and the legislation all include some sort of partnership or assemblage. It seems as the government realised that the private actors had the prominent role in the IT-industry and therefore also seemed to have the most knowledge regarding both how to operate it and also how to handle the challenges. However the government cannot force these private actors to share information nor can they expect these private actors to take the same responsibility as the public actors would. Possibly for these reasons there has emerged situations where there seems to have been some friction between the actors. As it concerns delicate matters, these possible frictions that may or may not exist between the actors involved in Sweden's cyber security, are probably not displayed for the public. The times when the frictions have surfaced it was the media and the journalists that exposed the truth. Hence there may or may not be more friction between the actors involved in the cyber security, however as it regards the national security, data regarding these possible frictions is hard to come by.

The use of the theory *Assemblage theory for cyber security* helped structure the study. Since it forces the researcher to thoroughly explain the development and the actors involved it was easier to understand the contemporary cyber security. Furthermore it proved, according to me, correct with the different shifts and captured the involved actors in a manner that painted a clear picture of Sweden's cyber security. However as mentioned, since my aim was to detect possible friction between the actors involved with special consideration towards the public-private sector, I chose to exclude the last shift. I believe that in order to fully test this theory it is important to include that shift as well. Furthermore in order to generalize the theory I also believe that it needs to be tested on more cases. Although according to this case study, with the exception of the fifth shift, the theory can be verified.

6. References

Abu Eid, Miriam (2017) “Regeringen föreslår en ny säkerhetsskyddslag”, *Regeringskansliet,* 16th November, https://www.regeringen.se/pressmeddelanden/2017/11/regeringen-foreslar-en-ny-sakerhetsskyddslag/ (Access date: 2019-05-20)

Acuto, Michele and Curtis, Simon (2014) “Assemblage Thinking and International Relations”. In: Acuto, Michele and Curtis, Simon (eds) *Reassembling International Theory*. Palgrave Pivot, London

Carr, Madeline (2016) “Public–private partnerships in national cyber-security strategies”, *International Affairs,* Vol 92, Issue 1, pp 43–62.

Christensen, Kristoffer Kjægaard and Petersen, Karen Lund (2017) “Public–private partnerships on cyber security: a practice of loyalty”, *International Affairs,* Vol 93, No 6, pp 1435–1452.

Collier, Jamie (2018) “Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision”, *Politics and Governance,* Vol 6, No 2, pp 13–2.

Dahlin, Niklas (2014) “Svenska Besk – världens snabbaste dator”, *NyTeknik,* 6th August https://www.nyteknik.se/teknikhistoria/svenska-besk-varldens-snabbaste-dator-6398561 (Access date: 2019-05-14)

Deibert, Ron and Rohozinski, Rafal (2010) “Cyber Wars”, *Index on Censorship,* Vol 39, Issue 1, pp 79-90.

Dobos, Lars (2019) “2,7 miljoner inspelade samtal till 1177 Vårdguiden helt oskyddade på internet” *Computer Sweden,* 18 February, *https://computersweden.idg.se/2.2683/1.714787/inspelade-samtal-1177-vardguiden-oskyddade-internet* (Access date: 2019-05-25)

DeLanda, Manuel (2019) *A New Philosophy of Society: Assemblage Theory and Social Complexity,* Bloomsbury Publishing Plc

Eichensehr, Kristen E. (2017) “Public-Private Cybersecurity”. *Texas Law Review.* Vol 95. No 3.

European commission (2018) “The Directive on security of network and information systems (NIS Directive”, *European Commission,* 24th August, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (Access date: 2019-05-22)

George, Alexander L and Bennett, Andrew (2005) *Case Studies and Theory Development in the Social Sciences,* Cambridge, Mass, MIT Press.

Goodin, Dan (2017) “NSA-leaking Shadow Brokers just dumped its most damaging release yet”, *Ars Technica,* 14th April, https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/ (Access date: 2019-04-23)

Grossman, Nadav (2017) “EternalBlue – Everything There Is To Know”, *Check Point Research,* 29th September, https://research.checkpoint.com/eternalblue-everything-know/ (Access date: 2019-04-23)

Internetmuseum (2019a) “1978 Ett svenskt socialt nätverk startas – det revolutionerande KOM-systemet”, *Internetmuseum: Internetstiftelsen,* https://www.internetmuseum.se/tidslinjen/kom-systemet/ (Access date: 2019-05-15)

Internetmuseum (2019b) “1980 Svenskarna kan prata via datorer även innan internet – med BBS”, *Internetmuseum: Internetstiftelsen,* https://www.internetmuseum.se/tidslinjen/bbs-kulturen-blomstrar/ (Access date: 2019-05-14)

Internetmuseum (2019c) “1995 Patrik ”Paf” Fältström – en internetagent i folkets tjänst”, *Internetmuseum: Internetstiftelsen,* https://www.internetmuseum.se/tidslinjen/patrik-paf-faltstrom-en-it-agent-i-statens-tjanst/ (Access date: 2019-05-14)

ITU (2019) “Definition of cyber security” *ITU: International Telecommunication Union,* https://www.iinttu./en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (Access date: 2019-05-24)

Johansson, Anders and Thornéus, Ebba (2019) “2,7 miljoner inspelade samtal till 1177 Vårdguiden helt oskyddade på internet”, *Aftonbladet,* 18th February,

https://www.aftonbladet.se/nyheter/a/5VXPm1/27-miljoner-inspelade-samtal-till-1177-helt-oskyddade-pa-internet
(Access date: 2019-05-25)

Levy, Jack S (2008) “Case Studies: Types, Designs, and Logics of Inference”, *Conflict Management and Peace Science*, Vol 25, Issue 1, pp 1–18.

Lönn, Ragnar and Schedin, Wilhemina (2016) ”Från Sundbyberg till Hötorget: Historien om Algonets början, fram till maj 1996”, http://www.acc.umu.se/~wschedin/ragnar.html
(Access date: 2019-05-15)

Löwenfeldt, Jörgen (2019) “Sammanfattningen: Den stora berättelsen om internets historia”, *Internetmuseum: Internetstiftelsen,*
https://www.internetmuseum.se/berattelsen-om-internets-historia/ (Access date: 2019-05-10)

McAleavey, Kevin (2011) ”The Birth of the Antivirus Industry”, Infosec Island, 11th July, http://www.infosecisland.com/blogview/15068-The-Birth-of-the-Antivirus-Industry.html
(Access date: 2019-04-23)

Ohlin, Jonas (2018) “Transportstyrelsen - Detta har hänt”, *SVT Nyheter,* 7th June,
https://www.svt.se/nyheter/inrikes/transportstyrelsen-detta-har-hant
(Access date: 2019-05-25)

Palme, Jacob (2015) “History of the KOM Computer Conferencing System”
https://people.dsv.su.se/~jpalme/s1/history-of-KOM.html (Access date: 2019-05-10)

Regeringskansliet (2017a) “A national cyber security strategy: Fact sheet”, *Regeringskansliet,*
https://www.government.se/4989ba/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy
(Access date: 2019-05-20)

Regeringskansliet (2017b) “A national cyber security strategy”, *Regeringskansliet,*
https://www.government.se/4ac8ff/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213
(Access date: 2019-05-21)

Regeringskansliet (2019) “Säkerhetsskyddslag (2018:585)”, *Regeringskansliet,*
http://rkrattsbaser.gov.se/sfst?bet=2018:585
(Access date: 2019-05-20)

Solms, von Rossouw and Niekerk, van Johan (2013) “From information security to cyber security”. *Computers & Security.* Vol 38. pp 97-102.

Statista (2019) ”Share of the population with access to the internet at home in Sweden from 2011 to 2018” Release date: Oktober 2018
https://www.statista.com/statistics/543324/sweden-access-to-the-internet/
(Access date: 2019-05-10)

Svete, Uroš (2012) “European E-Readiness? Cyber Dimension of National Security Policies1”, *Journal of Comparative Politics,* Vol 5, Issue 1.

Volz, Dustin (2017) “U.S. blames North Korea for 'WannaCry' cyber attack”, *Reuters,* 19th December,
https://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wannacry-cyber-attack-idUSKBN1ED00Q (Access date: 2019-04-23)

Warner, Micheal (2012) “Cybersecurity: A Pre-history”. *Intelligence and National Security.* Vol. 27, No. 5, 781–799, October 2012; Routledge

World Economic Forum (2019) “Global Risk Report 2019 14th Edition”, *World Economic Forum,*
http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
(Access date: 2019-04-20)

Zittrain, Jonathan (2006) The generative internet. *Harvard Law Review,* Vol 119, Issue 7, pp 1975-2040.