SOFT WAR IN CYBERSPACE

How Syrian non-state actors use hacking to influence the conflict's battle of narratives

Vivi Cathrine Ringnes Wilhelmsen

Master's thesis - Political Science
Department of Political Science
UNIVERSITY OF OSLO
May 2014

This page is intentionally left blank

SOFT WAR IN CYBERSPACE

How Syrian non-state actors use hacking to influence the conflict's battle of narratives

By Vivi Cathrine Ringnes Wilhelmsen

Master's thesis - Political Science

Department of Political Science

UNIVERSITY OF OSLO

May 2014

Spring 2014

Title: Soft War in Cyberspace- how Syrian non-state actors use hacking to influence the conflict's battle of narratives

Author: Vivi Cathrine Ringnes Wilhelmsen

http://www.duo.uio.no

Print: Reprosentralen, University of Oslo

Abstract

In Syria we see "cyber-armies", consisting of both pro- and anti regime combatant non-state actors, waging organized (dis-) information campaigns in cyberspace. Pushing an agenda of subversion, it is a different and more conflictual form of cyber-interaction then analyzed before. Moving from online media as an outlet and opinion-sharing platform, unauthorized alterations and manipulation resembles traditional disinformation and propaganda campaigns. One of the first of its kind, this phenomenon requires closer inquiry. The research question guiding the thesis is therefore: *"Why and how do non-state actors use cyberspace in modern conflict?"*. Underpinning the research question is several assumptions that will be evaluated in the case study. Firstly, we must establish that non-state actors use cyberspace as component in their conflict strategy. Secondly, this thesis is founded in the belief that they use it as a tool of subversion aimed at undermining their opponent. These "warriors" actively sabotage, persecute, and spy on each other and perceived supporters by hacking accounts, defacing websites and manipulating social media outlets. Both parties uses online media to "sell their story" to the domestic and global audience but they also actively use hacking as a tool in conflict and manipulate how events are perceived. Moving from (social) media as an outlet for opinions to active and unauthorized alterations resembles disinformation and propaganda campaigns.

Non-state actors use this domain in conflict situations to exploit it's potential for waging soft wars as a form of conflict participation where agendas and narratives compete. The third assumption is that they promote a strategic narrative and soft power through guerrilla tactics. The case study will illustrate that the ways of real world conflicts thus are adapted to cyberspace to attack the center of gravity in the opponent. This finding leads the conclusion that the cyber warriors seen in Syria is not a new phenomenon, simply the adaption of old strategies in a new domain. Lastly, the thesis operates under the assumption that the reach and effectiveness (measured in the level of attention and number of attacks) of the non-state actors depend on the level of organization and resources. These assumptions can be summarized in five points: These assumptions can be summarized in five points: (1) Non-state actors use cyberspace in conflicts; (2) Subversion is the ultimate goal of their actions in cyberspace; (3) This is done by spreading a strategic narrative and build soft power; (4) To reach their goal, they use guerrilla tactics; (5) The effectiveness is determined by level of

organization and resources. This thesis will combine literature on soft power and subversion within the framework of conflict in cyberspace. It argues that cyberspace gives non-state actors a new domain to undermine the role of the state or the opposition, but that neither the nature of conflict or the nature of subversion enters a new paradigm. Strategic narratives are used in the hope of shaping the relative soft power like in traditional conflicts. Combining an element of surprise, rapid movement, and sabotage these actors rectify their weaknesses, and promote a particular strategic narrative to alter the relative soft power balance. We therefore see a potential trend of "soft war" moving into cyberspace.

In this thesis the data collection is done by combining a targeted literature search with a large collection of primary data on attacks completed during the course of the Syrian conflict. One of the main contributions of this work is therefore an extensive empirical record of cyber attacks during the Syrian conflict. All attacks meeting the criteria[1] have been included in an attempt to provide as unbiased review as possible. This is presented in the appendix and forms the basis for the evaluation done in the analysis.

This thesis finds some support for all the assumptions, but naturally any soft element to conflict is complicated to measure during an ongoing conflict[2]. What is clear from the case study is that non-state actors use cyberspace extensively in the Syrian conflict. It is the most socially mediated conflict in history (Lynch, Freelon, and Aday 2014), and this domain still enjoys the perception as a channel for unmediated information. Manipulation and justifications are therefore key messages spread to undermine the adversary's position in the real world conflict. Ultimately they seek to subvert each other, aided by strategic narratives to shape the relative soft power balance. However, as they operate in an online maze and lack resources necessary for direct conflict, the actors studied use what can be called cyber guerrilla tactics. One of the actors studied, the Syrian Electronic Army (SEA), is rather successful in hindering information diffusion, implement espionage software, and infiltrate opposition online communication networks. The other party to the conflict, the opposition, is found however to have a much shorter empirical record and gains less attention. This is in great extent explained by their organizational proficiency.

[1] Non-state actors of a certain level of organization, presenting a strategy over some time. The findings of others are included to increase the legitimacy of the research.
[2] the Syrian case provides a new development in the role of non-state actors in cybered conflicts, it was deemed
[2] the Syrian case provides a new development in the role of non-state actors in cybered conflicts, it was deemed
the appropriate case As. This is further discussed later on.

Acknowledgements

Seven years of higher education is completed with this work. One bachelor, two masters, five universities and four countries later I am truly grateful for everything I have learned, all the people I have met, and for the possibility to make long journey. I would like to take this opportunity to thank all that has contributed to this thesis with discussions, insights, and patience during a long, exciting, and sometimes frustrating process. I truly enjoyed it, though learning the cyber language was somewhat of a challenge. I am especially grateful to my wonderful supervisors Øyvind Østerud and Torbjørn Kveberg, my family, and Peder. I could not have done this without your revisions and feedback, encouragement and hugs, and occasional friendly nudges.

Some of the ideas presented here have previously been introduced in term papers for the University of Oslo courses *STV4020 Research methods and statistics* and *STV4525B International Security Policy.*

All errors and opinions is the sole responsibility of the author.

Word count: 33 900.

Keywords: non-state actors in cyberspace, subversion and soft power, Syrian war 2011-2014, Syrian Electronic Army.

This page intentionally left blank

Content

List of figures and tables

Introduction

In Syria we see "cyber-armies", consisting of both pro- and anti regime combatant non-state actors, waging organized (dis-) information campaigns in cyberspace. Pushing an agenda of subversion, it is a different and more conflictual form of cyber-interaction then analyzed before. Moving from online media as an outlet and opinion-sharing platform, unauthorized alterations and manipulation resembles traditional disinformation and propaganda campaigns. One of the first of its kind, this phenomenon requires closer inquiry. The research question guiding the thesis is therefore: *"Why and how do non-state actors use cyberspace in modern conflict?"*. Underpinning the research question is several assumptions that will be evaluated in the case study. Firstly, we must establish that non-state actors use cyberspace as component in their conflict strategy. Secondly, this thesis is founded in the belief that they use the as a tool of subversion aimed at undermining their opponent. These "warriors" actively sabotage, persecute, and spy on each other and perceived supporters by hacking accounts, defacing websites and manipulating social media outlets. Both parties uses online media to "sell their story" to the domestic and global audience but they also actively use hacking as a tool in conflict and manipulate how events are perceived. Moving from (social) media as an outlet for opinions to active and unauthorized alterations resembles disinformation and propaganda campaigns.

Cyberspace also allows for the inclusion of more actors. Non-state actors use this domain in conflict situations to exploit it's potential for waging soft wars as a form of conflict participation where agendas and narratives compete. The third assumption is therefore that they do so to promote a strategic narrative and soft power through guerrilla tactics. The case study will illustrate that the ways of real world conflicts thus are adapted to cyberspace to attack the center of gravity in the opponent. This finding leads the conclusion that the cyber warriors seen in Syria is not a new phenomenon, simply the adaption of old strategies in a new domain. Lastly, the thesis operates under the assumption that the reach and effectiveness (measured in the level of attention and number of attacks) of the non-state actors depend on the level of organization and resources. These assumptions can be summarized in five points: (1) Non-state actors use cyberspace in conflicts; (2) Subversion is the ultimate goal of their actions in cyberspace; (3) This is done by spreading a strategic narrative and build soft power; (4) To reach their goal, they use guerrilla tactics; (5) The effectiveness is determined

by level of organization and resources. This thesis will combine literature on soft power and subversion within the framework of conflict in cyberspace. It argues that cyberspace gives non-state actors a new domain to undermine the role of the state or the opposition, but that neither the nature of conflict or the nature of subversion enters a new paradigm. Strategic narratives are used in the hope of shaping the relative soft power like in traditional conflicts. Combining an element of surprise, rapid movement, and sabotage these actors rectify their weaknesses, and promote a particular strategic narrative to alter the relative soft power balance. We therefore see a potential trend of "soft war" moving into cyberspace.

Some key developments form the framework of this thesis. Firstly, war has existed as long as humans have interacted in proximity[3]. However, how these are conducted has changed fundamentally over the course of history. Major wars like the American Civil War, the Russian Revolution, World War I and II, the Gulf War, and the War on Terror, are all milestones in the sense that they present key developments in how combatants organize and what technology is available (Diesen 2013). Since the end of the Cold War however, a growing percentile is intra-state conflicts. A key question has become why the weaker actors are able to defeat the stronger Goliath on so many occasions. One key conclusion is that non-state actors win when they refuse to follow the same strategy as the stronger party (Arreguin-Toft 2001)[4]. By defining and controlling the battleground, they are able to shape a strategy that plays to their strength, thus compensating for their weakness in numbers and sophistication.

Secondly, cyberspace and Information and Communication Technology (ICT) have rapidly become an integrated part of our everyday life and during conflict. Though of dubious direct military strategic relevance, as it is unable to settle a military conflict by itself, the perceived power of this domain is well illustrated by how governments in Iran, Syria and China have blocked oppositions' means of communication (Geiss 2013, 3). One interesting and new

[3] Today we see a wide range of conflict typologies; from low-intensity conflicts between groups in failed states like Somalia, through "traditional" civil wars seen in Syria, to internationalized conflicts like Afghanistan (Geiss 2013, 3)

[4] Arreguin-Toft's paper on why the weak win wars (2001) is an interesting, inspirational paper for this thesis. His study concludes that the weaker actor can be able to defeat the stronger *if* the strong and the weak use different tactics. If the stronger actor exploits its greater might by focused on direct attacks, the weaker is therefore advised to focus its strategy on the indirect, guerrilla-/ insurgency tactics to be able to survive and possibly increase its reach. By consequence one can therefore hypothesize that weaker actors using cyberspace as a tactical fighting ground may be able to have an impact on public opinion if left alone by the stronger state-actor.

perspective is Thomas Rid's (2013) book "Cyberwar will not take place". Rejecting the proposition that cyberspace fundamentally changes warfare and the potential of a "Cyber Pearl Harbor", Rid argues that the importance of cyberspace in conflict is in the potential for subversion, espionage and sabotage. This perspective is consistent with this thesis. It argues that cyberspace gives non-state actors a new domain in which to undermine the role of the state, but that neither the nature of conflict or the nature of subversion enters a new paradigm. Cyberspace only facilitates a new form of subversion as the nature of cyberspace is low-entry, allows the presence of many groups in conflict, and is global.

Thirdly, in the major conflicts of the last decades, winning "the hearts and minds" is presented as a panacea for sustainable stability and peace (Dickinson 2009). If so, cyberspace is likely to play a dominant role as a primary medium and influential tool. Additionally cyberspace is perceived as the "weapon of the weak", giving citizens a neutral medium to communicate among each other and to tell their stories to the world. Consequently the social-media revolutions are described as "people revolutions", linking massive online support to legitimate revolts. To what extent these beliefs that underpin for example the Arab Spring, are true is debated but online media holds potential for participants in a way impossible in traditional military domains[5]. The combination of perceived legitimacy and few obstacles to entry obviously makes alteration and manipulation of this domain attractive, much as propaganda and strategic communication in traditional media.

> Propaganda in the broadest sense is the technique of influencing human action by the manipulation of representations (Lasswell 1972, 214–222).

In this thesis the data collection is done by combining a targeted literature search with a large collection of primary data on attacks completed during the Syrian conflict. One of the main contributions of this work is therefore an extensive empirical record of cyber attacks during the Syrian conflict. All attacks meeting the criteria[6] have been included in the attempt to provide an as unbiased review as possible, though some limitations are discussed in the methodology chapter. The record of the primary data is presented in the appendix, and forms

[5] If accepting that cyberspace is a conflict domain one must also accept that it is lower entry barrier than say traditional warfare on land, sea or air due to the level of resources necessary. However, high impact cyber campaigns like Stuxnet does not have the same low barrier as the cyber operations evaluated here. This type demands massive resources, human capital and intelligence and is therefore beyond the scope of the groups evaluated here. Additionally there is the open-source nature, the potential for anonymity and global reach.
[6] Non-state actors of a certain level of organization and presenting a strategy over some time.

the basis for the evaluation done in the analysis. The findings of others are included when relevant to increase the legitimacy of the research.

This thesis finds some support for all the assumptions, but naturally any soft element to conflict is complicated to measure during an ongoing conflict[7]. What is clear from the case study is that non-state actors use cyberspace extensively in the Syrian conflict. It is the most socially mediated conflict in history (Lynch, Freelon, and Aday 2014), and this domain still enjoys the perception as a channel for unmediated information. Manipulation and justifications are therefore key messages spread to undermine the adversary's position in the real world conflict. Ultimately they seek to subvert each other, aided by strategic narratives to shape the relative soft power balance. However, as they operate in an online maze and lack resources necessary for direct conflict, the actors studied use what can be called cyber guerrilla tactics. One of the actors studied, the Syrian Electronic Army (SEA), is rather successful in hindering information diffusion, implement espionage software, and infiltrate opposition online communication networks. The other party to the conflict, the opposition, is found however to have a much shorter empirical record and gains less attention. This is in great extent explained by their organizational proficiency.

Previous research is limited, and mostly focuses on the use of social media by citizens or cyber wars between states. This thesis however studies the use of hacking by non-state actors in an information warfare perspective. This thesis does not seek to develop any theory, only provide more insights into the Syrian groups. The key outcome is therefore an attempt to develop an analytical framework, and the collection of an extensive record of the attacks completed by the Syrian cyber warriors[8]. Hopefully, it will also indicate a course of research that can be adapted to other cases in future research. A sure academic footing is vital when undertaking a work such as this, but before the theoretical framework can be presented we need a clear understanding of technological aspects in the thesis and of the key terms. Then the foundation for the guiding assumptions and theoretical groundwork will be presented. A methodological chapter will then outline the choices made, the guidelines implemented for

[7] the Syrian case provides a new development in the role of non-state actors in cybered conflicts, it was deemed the appropriate case As. This is further discussed later on.

[8] The author has followed the groups from 2011 to 2014, and has recorded all the attacks reported in international media available at the time of writing. Though some shortcomings may exist, 106 attacks are recorded and analyzed. Additionally are attacks verified by other researchers but not included in the primary data due to the fact that the author has not seen primary proof of the attack. To my knowledge, this thesis therefore provides one of the most comprehensive records, especially in the case of the SEA.

the primary data collection, and the strengths and weaknesses of the research project. The case study of Syria will then follow, testing the assumptions against empirical findings. Lastly conclusion will be presented at the end of the work.

The basics of cyberpower: type of attacks and key terms

Cyberpower is a new conception, and is recently incorporated into the growing literature on cyber warfare. Unfortunately, many understandings of key terms and academic assumptions thus exist. Additionally this thesis is written as a partial completion of a master program in political science, and readers may not be familiar with relevant nuances to technological concepts. This section outlines key terms and how possible attacks can come about. The description will be as non-technical as possible[9].

The basis of all cyber behavior is based in what networks enable; that two or more computers can communicate. This is the foundation for any of the attacks evaluated here, as the attacker uses his/ her computer to manipulate the victim's to do its biddings. When two or more networks communicate, they create an "ant hill" of integrated information systems. They can be closed, which means that they exist within a defined area and is usually referred to as "Intranet". These can be global but have a more limited reach as they do not link onto the global "cyber-highway" we call the Internet. Networks that are a part of this global infrastructure however are referred to as open. The cyber actors analyzed in this research are of rather low sophistication and have yet to attack a closed network, which is by nature harder to access. Therefore, this will not be evaluated.

Non-state actors in cyberspace can refer to a number of actors, ranging from civil personnel working with infrastructure, criminals exploiting software weaknesses, hacktivists pushing a cause, to "cyber warriors". Distinction is complicated and often blurred as jurisprudence is still immature, academic classification disputed, and actors often cross imaginary boundaries between the various "professions[10]". The type of actors studied in this work must have a political agenda in the conflict, some sort of organization, be formally independent of any government, and have completed several attacks.

[9] As the analysis is of a political science nature, all technological aspects are also not necessary and can be accessed in the vast IT literature.
[10] For example: how to classify a youngster causing damage to a website due to weakness in Wordpress code for "fun"? Or hacktivist group Anonymous? Or differentiate between the recruitment process online for the mentioned groups and collectives vs. Terrorists?

When networks are interlinked and communicate, they create cyberspace. Though an everyday concept, it has various meanings depending on a materialistic (hardware), infrastructural (linkage), or effect based (software) focus. The fact that the environment is manmade further complicates the understanding and I have therefore included a brief definition:

> Cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems (Ottis and Lorrents, 2010:267). It is the notional environment where digitalized information is stored or communicated over information systems or networks (Hunker 2010, 2).

Cyber power therefore becomes:

> The ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power. Cyber power can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace. Information instruments can be used to produce soft power in cyber space through agenda framing, attraction or persuasion (Nye 2010, 3–5).

As we see, it can be further divided into soft and hard cyber power. While hard power rests on coercion and payment, soft power behavior relates to framing agendas, attraction or persuasion (Nye 2004 ch.1). Soft power, therefore, changes behavior by shaping preferences and what is deemed legitimate (Nye 2010, 8–9). Joseph Nye further divides cyber power into "three faces" and concurring actions[11]:

[11] David J. Betz and Tim Stevens have similarly classified four types of cyberpower (Langø 2013a, 28–29): a) compulsory, b) institutional, c) structural, and d) productive[11]. The most relevant for this thesis is productive power, defined as "the constitution of social subjects through discourse mediated by and enacted in cyberspace, which therefore defines the 'fields of possibility' that constrain and facilitate social action"(referred in Langø 2013a, 28–29).

Table 1: The three faces of cyberpower (Nye 2010, 7)**.**

1st Face: A induces B to do what B would initially otherwise not do		
	Hard Power:	Denial of service attacks, insertion of malware, SCADA disruptions[12], arrests of bloggers.
	Soft Power:	Information campaigns to change initial preferences of hackers, recruitment of members of terrorist organizations.
2nd Face: Agenda control: A precludes B's choice by exclusion of B's strategies		
	Hard Power:	Firewalls, filters and pressure companies to exclude certain ideas and behaviors.
	Soft Power:	ISPs[13] and search engines self monitor, ICANN[14] rules on domain names, widely accepted software standards.
3rd face: A shapes B's preferences so some strategies are never considered.		
	Hard Power:	Threaten to punish bloggers who release certain material.
	Soft Power:	Information to create preferences (e.g. nationalistic patriot hackers), develop norms of revolution (e.g. child pornography).

Cyber attacks of varying impact are completed to project cyber power. Repeated cyber attacks between two or more parties can thus be understood as the foundation of a cyber conflict. Cyber conflict is defined by CCSA research agenda (2005) as:

> The conduct of large scale, politically motivated conflict based on the use of offensive and defensive capabilities to disrupt digital systems, networks and infrastructures, including the use of cyber-based weapons or tools by non-state/transnational actors in conjunction with other forces for political ends. Broader then cyber warfare, cyber conflict includes all conflicts and coercions between nations and groups for strategic purpose utilizing cyber space where software, computers and networks are both means and targets (referred in Mulvenon and Rattray 2012b, x).

Cyber attacks consist of identifying weaknesses in systems and inflicting damage by altering

[12] A system operating with coded signals so as to provide control of remote equipment. May be combined with a data acquisition system by adding the use of coded signals to acquire information about the status of the remote equipment for display or for recording functions (Cyber Security Dictionary 2012).
[13] An Internet service provider (ISP) is a company that provides customers with Internet access (Janssen n.d.).
[14] The Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the Internet Assigned Numbers Authority (IANA) functions, which are key technical services critical to the continued operations of the Internet's underlying address book, the Domain Name System (DNS) (ICANN n.d.)

how the system works, much like biological viruses (T Chen and J.M. Robert 2004, 1). The former relates to behavior like copying or removing data without permission, but without disrupting the original architecture of the system. Consequently an active attack refers to operations where systems are corrupted or disrupted, and service is affected or denied (Hunker 2010, 2). Computer Network Attack (CAN) is one sub-type and refers to either action undertaken to disrupt, degrade, deny or destroy information stored on computers or in networks, or manipulate and/ or take control over a computer or network[15]. This is the type of cyber attacks studied in this work[16]. It is also possible to distinguish based on purpose between information warfare, which targets diplomacy and propaganda, and cyberwar founded in military operations targeting IT infrastructure. One can therefore distinguish two categories of cyber attacks; those that affect the physical world (Geers 2011, 41) and those with a "softer side"; aimed at perception management, deception, or any form of psychological operations (Mulvenon and Rattray 2012a, xii). Though not an end itself, cyber attacks are means to a wide variety of strategies like propaganda, espionage, denial of services, and disruption of infrastructure (Geers 2011, 9).

There are also multiple tools of cyberpower. Some, like Stuxnet[17], are of high sophistication and requires vast resources and intelligence. Others can easily be done with free software found online. The tools used by the actors in this research lean towards the lower levels. Though a learning curve is expected, it is more likely that they will use the same type of attacks on victims of higher importance. Below is a brief introduction to the tools of cyber power most relevant to this thesis:

- SQL injection[18]: More commonly known as hacking of computer systems, social media accounts or a website. SQL injection is a rather technical term but signifies that unauthorized actors access the backdoor functionality of for example web applications or user-supplied data. Unauthorized individuals thus change the

[15] Targets can involve states, commercial enterprises or individuals (Sheldon 2013, 311).
[16] Electronic (where electro-magnetic pulses overload circuits) and physical attacks on infrastructure are excluded from this analysis. This is known as Computer Network Operations (CNO), which embodies CND (Computer Network Defense) CNA (Computer Network Attack) and CNE (Computer Network Exploitation). CNA refers to attacks where damage is caused within or with help from the system. CNE refers to espionage where information is taken without permission.
[17] Stuxnet was a computer worm discovered in 2010. To date it is the most sophisticated, and is believed to have targeted the Iranian nuclear program. It collected information and damaged centrifuges by increasing their speed. It consisted of a highly specialized malware and is believed developed by the US or Israel's national security agencies.
[18] SQL is the abbreviation used for structured query language, but it is more common to just use the abbreviation.

architecture to fit their preferences. It subverts the original intent of the application by altering the statements controlling functionality. It can also be used to distribute malware to users of the application (Sammut and Schiffman 2014).

- Denial of Service Attacks (DoS): a type of attack on a network seeks to overload its capacity with activity, and thus forcing the network to crash[19]. A large-scale version is Disruption and Denial of Services (DDoS) where multiple compromised systems, which are usually infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.
- A Botnet (= "net of robots") is a collection of network-linked programs that communicate with other programs to jointly solve a task. It is often done by machines[20], and facilitates large-scale spamming of commercials or to facilitate DDoS. Certain software can link multiple computers together and thus strengthen the capacity of an attack; this is done by so-called "zombie computers[21]".
- Defacement can be understood as a form of cyber vandalism. It means that a hacker accesses a website and alters the information stored here, usually by SQL injection. Often they leave some type of signature, like a logo, to prove that they accessed the site much like graffiti in public places.
- Surveillance systems like Remote Access Trojan (RAT). RATs are usually downloaded with a software update or email attachment (Rouse 2009). It gives administrative control, which allows the intruder to a) monitor user behavior through keyloggers (which steals passwords) or other spyware; b) access confidential information, such as credit card and social security numbers; c) activate a system's webcam and record video; d) take screenshots; e) distribute viruses and other malware; f) format drives; g) delete, download or alter files and file systems. When the system is compromised, RAT also facilitates spread of malware to for example establish a botnet (Rouse 2009).

[19] One way of thinking of this effect is to imagine a highway that suddenly experience unprecedented traffic, and extensive traffic jams develop. However in cyberspace, the non-physical element, this leads the highway to collapse much like a overloaded bridge.

[20] There are some records of this being done by individuals refreshing specific sites or forwarding emails in a coordinated manner. This may cause overload, but is relatively ineffective as it is highly labor intensive compared to an automated network of computers working together. Additionally the computers are able to operate faster, thus creating more traffic than humans are able to do, and therefore hold a higher potential for success.

[21] These referrers to compromised computers, which are controlled by hackers or other, unauthorized individuals.

- Software like VPNs and Proxy Servers obscure identity. Virtual Private Network (VPN) increases the reach of a private network by connecting it through public networks like the Internet. By creating a “tunnel” it enables computers to exchange data as if they were located within the same closed network. Proxy server is when one machine operates as an intermediary between two others. Using this type of software can therefore obscure location and identity. It may also be a way of bypassing firewalls or access restrictions

After this clarification we will now move on to the next chapter of the thesis, outlining the theoretical basis of the research that underpins the described research question and key assumptions.

Theory and literature review

There are several key assumptions underpinning this research project. They will be tested at length in the case study, but beforehand the analytical and theoretical framework must be presented and past research evaluated. Firstly we will evaluate the reality of cyber warfare as this debate creates the analytical backdrop of the thesis. It also explains much of the definitional confusion and why non-state actors are overlooked as a topic within this strain of research. It clarifies the evolution of the field and thus becomes a key component of a literature review. The second sub-chapter will take a closer look at what guerrilla tactics entail and how these can be translated into cyberspace. Thirdly, the role of the non-state actor in this domain will be outlined. Lastly, two sub-chapters will draft the relevance and meaning of narratives and soft power. It will demonstrate how informational and psychological warfare have kinetic, subversive effects and how these manifest in cyberspace. Together these sub-chapters form the base of the thesis.

Is cyberwar coming?

Academics have since the 1990s claimed that the integration of cyberspace into conflict has fundamentally changed how wars will be fought (Geers 2011, 9, 25). According to Mulvenon and Rattray:

> Cyberspace has altered politics, economics, social interaction, national security and provided new opportunities, capabilities, vulnerabilities and threats (2012a, vii).

In 1993, cyberwar was declared imminent by Arquilla and Ronfeldt[22], and became a common phrase in national security by the end of the millennium. Simultaneously our growing dependence on IT systems to provide basic services to the citizenry also led to concerns of cyber-terrorism. Security personnel feared being held hostage by rouge actors with unauthorized access to vital national infrastructure, and responded by establishing cyber armies and cyber militias[23]. Though of more recent date, these sentiments is well illustrated in a quote from Geers (2011, 105):

[22] Arquilla, John, Ronfeldt, David F. and Rand Corporation. (1992), *Cyberwar is coming!* Santa Monica, California: RAND

[23] For example USA, Norway and Estonia now have integrated cyber units in their military.

> A cyber attack is best understood not as an end in itself, but as an extraordinary means to accomplish almost any objective. Cyber propaganda can reach the entire world in seconds via online e news media. Cyber espionage can be used to steal even nuclear weapons technology. Moreover, a successful cyber attack on an electrical grid could bring down a myriad other infrastructures that have no other source of power.

Over the last couple of years, the debate has somewhat shifted. Though still state-centric, some recent works conclude that the probability of a "Cyber Pearl Harbor" is grossly exaggerated (Langø 2013b, 5)[24]. In "Cyberwar will not take place" (2013) Thomas Rid argues that cyberwar cannot become reality, as the domain is unable to cause violent effects. Eric Gartzke further argues that conflicts in cyberspace are unable to deter or compel the opponent in the physical world, and thus has little independent value (Langø 2013b, 21). It does not correspond with Clausewitz' three criteria of war[25], and can only be understood as sophisticated versions of traditional tactics like sabotage, espionage and subversion (Rid 2013). Instead of changing war itself, it only adds another dimension to fight in.

The empirical evidence supports this argument; cyber incidents tend to follow actual conflicts as the Chechen wars during the 1990s, the Kosovo war in 1999, the Middle East in 2000, Estonia in 2007, and Georgia in 2008 (Geers 2011, 80–86). The attacks have a broad specter of targets, and seek to impact whatever economic, informational or propaganda aspects of the conflict possible[26]. As the effects are at best uncontrollable and questionable, the costs of developing sophisticated cyber weapons are not worth the benefits. The framework of this thesis thus operates with a middle ground of cybered conflicts; where kinetic and virtual tactics interact to a common approach. Here low-level cyber attacks are used as a complementary strategy to the real conflict, but resembling traditional vandalism, propaganda, or sabotage. Therefore there are to date no cyber wars, in the sense that conflicts are not fought exclusively with cyber power.

[24] Thomas Rid and David J. Lonsdale spearheads this perspective (Langø 2013a, 15), which also guides this thesis.
[25] Instrumental, political and violent (Rid 2013, 1)
[26] For example during the Georgian conflict (2008), Russian hackers targeted government websites in hope of hampering coordination between agencies and damage the citizenry's faith in its government. The success of these attacks is debated due to complications in measure effects. Also in Estonia the same trend was reported. For example, Ruus concludes that "the wave of attacks in Estonia, targeted the entire civil and economic infrastructure with the aim of paralyzing the society in a country, whose high reliance on computerized networks has given it the nickname "E-stonia" (Ruus 2008). To date there are no record of decisive military effects, though there are some claims that Israel was able to enter Syrian airspace undetected in 2007 due to a cyber intrusion.

What is a non-state actor in cyberspace?

Unfortunately, there is not much previous research relating to the non-state actor in cyberspace as most focuses on the state behavior. However, there are several push factors explaining the entry of non-state actors in cyberspace, ranging from the architecture of the infrastructure to the social components of this domain[27]. Additionally, recent conflicts indicate that non-state actors' reach and importance in this domain is only growing[28].

The Oxford Dictionary describes a non-state actor as "an individual or organization that has significant political influence but is not allied to any particular country or state" (2014). Academically, non-state actors can thus be defined as "an organized political actor not directly connected to the state but pursuing aims that affect vital state interests" (Pearlman and Cunningham 2012, 3). They can therefore include all "non-governmental actors who are participants in conflict including terrorists, protest groups, criminal organizations, corporations, multi-stakeholder organizations, ad-hoc collaborative groups and individuals" (Mulvenon and Rattray 2012a, 88). Non-state actors in this thesis refer to the individuals operating outside the governmental establishment to reach a political goal. Thus their behaviors work in collaboration (of a certain formality) with their chosen political group. The group refers to either the established regime or its' contenders[29]. If supporters of the regime, non-state actors refer to groupings working to maintain the regime's authority despite not being part of the formal structure[30].

> The involvement of civilians in recent cyber-conflicts has created a sizeable gray area between hacktivists, political hackers and legitimate combatants backed by nation-states. The debate has been fierce concerning if these people are individual and independent actors, motivated by political or nationalistic goals, or participants in covert government-orchestrated campaigns with the purpose to further the strategic political or military objective of the instigating state (Sigholm 2013, 22–23).

[27] As we will see, the low barrier to entry (at least for low level attacks and vandalism) allows more actors than in traditional domains of war. Also important to keep in mind is the global reach of the internet, again allowing more actors. Thirdly, unlike traditional domians, in cyberspace most of the infrastructure is privatley owned and operated. This allows for a new level of private expertise and insights than seen before.

[28] In both the conflicts in Estonia and Georgia, non-state actors lead the offense and defense in cyberspace (Ottis 2010; Ruus 2008).

[29] In the case of Syria, there are multiple rebel groups and insurgent coalitions who cooperate to a changing degree. However, these insurgents are included in the described understanding as they are political actors whom challenge the regime by political and military means.

[30] Here I refer to police, military or militias. To exclude various non-governmental groups like humanitarian agencies, lobbying organizations and various NGOs, the non-state actors dealt with in this research project undergo their tasks with the purpose of either maintaining or overthrowing the current societal structure, and their operations are part of a greater military strategy. As the thesis do not study government agents, like the intelligence apparatus, individuals belonging to this group are also excluded.

Non-state actors will remain a crucial part of future conflicts, and it is likely that this transcends into cyberspace; Mulvenon and Rattray even describes them of special relevance vis-à-vis other actors (Mulvenon and Rattray 2012a, 85). There are several reasons for this, but the underpinning assumption is that certain variables push the entry of such actors into the cyber domain, where they may have greater effects than in the physical world. The main push factors are: a) there is a low cost of entry compared to the other domains of war, despite the high expertise necessary to yield military results; b) by consequence the number of actors is in theory indefinite; c) nothing is final in cyberspace and multiple spaces can exist simultaneously; and d) the time and space dimensions are smaller than in reality (Sheldon 2013, 210); e) the barrier to entry in cyberspace is relatively low, at least if the goal is attacks of low sophistication; and f) geographical factors do not necessarily dictate the parameters of actions as all are equally distanced from each other and hard- and software compose the environment. The real distinction in power is therefore based in innovation and logic, not traditional strength (Geers 2011, 10). Cyberspace's anonymity also blurs the distinction between state and non-state actors[31], and government and civilian targets (Mulvenon and Rattray 2012a, 91). Regardless, Dorothy Denning concludes that the presence of, and possible dominance of cyberspace by non-state actors is too simple an argument. She agrees that the basic elements like computers and developing malware is rather simplistic compared to traditional military infrastructure. But any cyber attack with a "punch" is not easily done, and may come with a higher costs and more dubious outcome than in traditional conflict (Langø 2013a, 22)32. It is consequently more likely that the weaker actors will use methods of low sophistication, without the purpose of yielding definite results as described in the sub-chapter relating to guerrilla warfare.

[31] As discussed there are several types of software that enables hiding ones' identity. Secondly there is no way of seeing if a person behind a screen is wearing a uniform. Thirdly, cyber actors are often only known by their screen names and can in theory be of any gender, race, age, religion and nationality.
[32] DDoS and web-defacement is low barrier, but it is questionable if the effects can be significant.

Guerrilla warfare as a strategy in conflict

Any form of conflict between parties with diverging resources has an asymmetrical nature. An asymmetrical conflict strategy can be thus be defined as:

> Leveraging inferior tactical or operational strengths against the vulnerabilities of a superior opponent to achieve a disproportionate effect with the aim of undermining the opponent's will in order to achieve the asymmetrical actor's strategic objectives (McKenzie Jr. 2001, 75–76).

Guerrilla warfare is a form of asymmetrical strategy, where the weaker combatants exploit its advantages to make up for its shortcomings in brute size and force. By avoiding direct conflict while imposing great costs, the guerrilla warrior hopes to raise the opposition's stakes to an unacceptable level. Guerrilla warfare strategy is the organization of a proportion of society for the purpose of imposing costs on an adversary using armed forces trained to avoid direct conflict (Arreguin-Toft 2001, 103). It primarily targets opposing armed forces and their resources. It's goal is to destroy not the capacity, but the will of the attacker (Arreguin-Toft 2001, 103). By doing so, the warrior seeks to end the conflict on more favorable terms than its relative position indicates (Arreguin-Toft 2001, 103) [33]. Thus they are complementary to regular forces, not decisive independently (Kalyanaraman 2003, 177). It is defined as:

> Guerrilla warfare is a form of warfare by which the strategically weaker side assumes the tactical offensive in selected forms, times, and places (Kalyanaraman 2003, 172).

Usually including insurgents, the non-state actors can be either in conflict against, or collaborate with, states (Mulvenon and Rattray 2012a, 88). The defining characteristic, therefore, is that the actors function with different capabilities and relative power, and by consequence different rules and realities. The state will hold the greatest traditional resources, and the insurgents are forced to choose untraditional strategies to survive. By refusing to play the game of the stronger party, David may ultimately be able to defeat Goliath. Colonel

[33] Ivan Arreguin-Toft (2005) actually finds that non-state actors succeed to a surprising extent. However the key variable in determining the winner is, according to Arreguin-Toft's study, if the two parties chose the same or different strategies. Similar approaches favor the stronger as this dominates its chosen battlefield, while different strategies allows the weaker party to elect a responses that favor their strengths and exploits the stronger party's vulnerabilities (Arreguin-Toft 2001, 108). One element of Arreguin- Toft's thesis is however less relevant this analysis. The thesis claims that the weaker party can be more barbaric than the stronger, and thus plays by other rules. As cyber conflicts to date have had no direct casualties, this part of Arreguin-Toft's thesis cannot be empirically tested. Arreguin-Toft distinguishes between direct and indirect tactics. The former targets the capacities of the attacker, while the second targets the will. Use of the same strategy favors the strong actor, while opposite approaches favor the weak (Arreguin-Toft 2001, 105).

Wallace and Major Reeves provide us with an amusing illustration of how this results in two realities of conflict strategy:

> In a fight between a fly and a lion, the fly cannot deliver a knockout blow and the lion cannot fly. It is the same war for both camps in terms of space and time, yet there are two distinct types of warfare – the revolutionary and the counterrevolutionary (Wallace and Reeves 2013, 2).

As in the physical world, non-state actors use cyberspace's terrain, mobility, and special tactics to "turn the tables" on the stronger actor. This form of behavior may allow the groups to overcome their relative weakness compared to state militaries, as traditionally seen in guerrilla, raiders and insurgents warfare (Mulvenon and Rattray 2012b, 89). Insurgents avoid direct confrontation with the counterinsurgents, using hit-and-run violence, and utilizing small irregular groups to secure preservation (Findley and Young 2007, 383). It distinguishes from conventional warfare by lacking a clear front-line and large-scale, set-piece battles. Modern guerrillas also tend to be intensely focused on propaganda, swaying public opinion and winning the battle of the narrative by wearing down the enemy (adapted from Boot 2013, xxvi, xxii). Taber illustrates the strategy of guerrilla warfare with an interesting image:

> The guerrilla fights the war of the flea. The flea bites, hops, and bites again, nimbly avoiding the foot that would crush him. He does not seek to kill his enemy at a blow, but to bleed him and feed on him, to plague him and bedevil him, to keep him from resting and to destroy his nerve and his morale (Stout 2009, 881).

Logically this form of waging war is adaptable to cyberspace. By exploiting and manipulating the architecture of this man-made environment, the actors turn their weaknesses to strengths. As in the real world, it is impossible for the stronger party to defend "everywhere" at all times. Thus, the weaker party can use hit and run tactics to attack the weaker point, whatever that might be. As guerrilla warriors attack a wide range of targets, the cyber actors have a broad specter of marks and are not by geography[34]. In cyberspace, this would entail using simpler forms of attacks against the weakest points, like sabotage and vandalism of whatever of websites with lesser consideration to their strategic importance. In traditional conflict, guerrilla warriors depend on light weaponry as a part of a strategy of denial instead of a strategy of defeat[35] (Kalyanaraman 2003, 173). This thesis argues that low sophistication attacks are the cybered version of this strategy, executed to attack the will of

[34] Though some locations have better infrastructure. However, in this case the actors of both factions mostly operate outside of Syria and thus in the same geographical location.
[35] As discussed bellow, the weaker guerrilla warrior cannot defeat the stronger party and thus focus their effort on raising costs to an unacceptable level.

the opponent.

The mentality of the non-state actors in cyberspace also resembles the of traditional guerrilla warriors. They use the element of surprise and terror to their advantage, making anyone a potential target. Secondly, anonymity is embedded in the structure of cyberspace. Following the doctrine of Mao Zedong, the cyber warriors are becoming "the fish in the water" and indistinguishable from civilians. By attacking from the shadows, they need not fear retaliation (Toor 2011). They use ambushes and sabotage instead of open confrontation. The cyber-guerrillas can see the state clearly; the state cannot see them (Mavhunga 2008). These "flee bites" seek to provoke harsh retaliation by the opposing party, creating sympathy and recruit new supporters. The cyber guerrilla, as in the real world, benefits from the fact that the state is less able to respond quickly and restricted by rules and regulations.

Traditionally guerrilla warfare is used when non-state actors fight the state. However, it is important to keep in mind that both factions studied here are defined as weak. Thus the stronger party, making the conflict asymmetrical, is a result of them operating outside the state system while attacking more resourceful third parties[36]. Additionally there is a relative power balance between the two factions of the cyber conflict. Regardless, the definitions and tactics are applicable when the weaker (pro- and anti-regime actors) use the benefits offered by the domain (cyberspace) to take on the relatively stronger actor (the Syrian state and the international community). In sum, we see that the guerrilla model's power relationship applies. Lastly, as in real world guerrilla warfare the goal is ultimately to weaken the enemy's will and not inflict offensive loss. Asymmetric warfare is, therefore, understood as a strategy, a tactic, or a method of warfare and conflict[37] (Grange 2000, 1), both in the real and the virtual world.

[36]. In this case study, this refers to international news organizations or foreign governments / individuals.
[37] Three prominent examples of asymmetric actions that counterbalanced established force are: the sturmtrupp assault tactics that broke the trench-line stalemate and three-dimensional warfare as a result of the airplane during World War I; the panzer blitzkrieg through France in World War II; and the Strategic Defense Initiative that helped end the nuclear arms race between the U.S. and the Soviet Union. The kind of asymmetric strategy and tactics seen in the Vietnam War were termed guerrilla warfare (Quote Grange, 2000:1).

The power of the perspective

Modern wars are different from those of the past, as they relate to the breakdown of a state unlike the former state-building wars (Kaldor 2013, 3). The source of conflict is thus, to a growing extent, "identity factors" (Kaldor 2013, 3) where the combatants represent different factions of a society. Consequently the non-state actor is a key player in conflicts, which often take place within the state. The key actors are hard to identify as they participate due to a number of motivations[38], tendencies and interests (Kaldor 2013, 12). Political in nature, these loose networks are connected through overreaching narratives, which build a common identity. A key component of these conflicts are, therefore, informational and psychological warfare. Asymmetrical strategies are used to build legitimacy and support to compensate for physical and relative weakness. Both new and traditional media are therefore exploited and manipulated to push the chosen cause, and Syria illustrate that cyberspace is becoming a favored domain for the weaker party in a conflict to "win the hearts and minds".

Any discussion relating to conflict has an embedded debate on "power". Power is a multifaceted term, but the traditional meaning signifies that person A can make person B do something (s)he would otherwise not do. What qualifies as power will therefore always depend on the surroundings and context (Nye 2010, 1) but it can generally be understood as the "ability to influence the behavior of others to accomplish the outcomes one wants"(Nye 2004, 5)[39]. Power was later reorganized into two groups; hard and soft power by Joseph Nye. Hard power behavior rests on coercion and payment, while soft power behavior rests on framing agendas, attraction or persuasion (Nye 2004 ch.1). Soft power thus describes how external persuasion can alter behavior, creating the same gains without resorting to force and threats (Nye 2010, 8). It revolves around framing and altering what is seen as important (agenda-setting) and, in its outmost extent; change another person's preferences. Soft power therefore relates to what extent the influenced actor sees its own actions as legitimate (Nye 2010, 8–9). If so, the agenda setting has resulted in a "soft power-hold", imaginable both stronger and more enduring that any forced behavior.

[38] Like ideology, religion, culture, zelotry or economic gains (Grange 2000, 2)

[39] From the 1950s to the 1970s nuances were established through the "three faces of power"; a) getting others to do what they would not otherwise do (e.g. Robert Dahl, 1950s); b) agenda setting, or framing issues in such a way that the issue of coercion never arose (e.g. Peter Bachrach and Morton Baratz, 1960s); and c) that ideas and beliefs also help shape others' preferences, and one can also exercise power by determining others' wants (e.g. Steven Lukes, 1970s) (all refered in Nye 2010).

To frame others to operate in a manner of your choice without coercion is obviously very attractive as it demands fewer resources and provides a great pool of beneficial assets. Strategically it also allows for long-term victories, sustainable long after the military confrontation is over as "the hearts and minds" are conquered. This is not a new idea. Clausewitz saw warfare as an extended duel to "comply the enemy to do our will" (Berger 2013). Obviously this is also the goal of the non-state actors in cyberspace. Throughout *the Art of War*, Sun Tzu highlights the importance of information and perception (deception and surprise) as the foundation for all military strategies and tactics (Berger 2013). Mao, inspired by Sun Tzu, even developed a philosophy of the importance of guerrilla tactics and non-state actors principles of behavior. Here the key was to become "the fish in the sea"; where it impossible to differentiate between the population and the rebels. As cyber activities cannot determine conflicts independently, its lure becomes the reach and persuasion in winning the "people", "the battle of the narrative" and ultimately "the soft war". It shares many similarities with Bordieu's "power to construct social reality" (O´Hagan 2013, 559). To quote Grange: "The infosphere has become a new battleground suited for asymmetric attack from across the globe"(Grange 2000, 3).

We know there is a linked relationship between beliefs and feelings (cognition and attitude) and action (behavior), but we are yet unable to quantify the effects (Leuprecht et al. 2010, 47). However, we see that narratives target the two former, and use the impression made here to push for a certain type of action. Narratives "channel ideology, express collective identity, provide reason for action and aid in interpreting others" (US Army Field Manual 3-24, Counterinsurgency, cited in Zalman 2010, 4). Building on past and present (perceived) grievances and in-/out-group mentality, the storyteller justifies a certain form of behavior and entices others to follow. Personal connections and loyalties are promoted, and the group becomes a source of protection and safety (Leuprecht et al. 2010, 48–49). A strategic narrative can thus be understood as "system of stories that share common themes, forms, events, and participants, and create expectations for how those elements can be assembled to satisfy a desire that is rooted on conflict"(Nissen 2013, 73). By targeting the attitudes and perceptions, the sender seeks to control the behavior of others. Casebeer and Russel claims that the undermining of the opposing narrative can in the end decide the level of support and thus have kinetic effects in traditional warfare (Bøe-Hansen 2010, 24). However this strategy requires the attention of the recipients, and media thus becomes a powerful channel for

presenting one's narrative.

> People only know a little region of their social lives; their beliefs and loyalties lack deep traditions. They are vulnerable to rumors, news and trends. Media is therefore used to make sense of a confusing, obscure and shifting world (Gitlin 2003, 1).

The relationship between media and politics is defined by the media's potential to form social understandings of the world, attitudes towards others, and how we comprehend conflicts (O´Hagan 2013, 558). Media and information becomes a tool of mobilization and persuasion; where all parties tell their "strategic narrative[40]" to promote a certain political behavior (Nissen 2013, 73). Media, through the CNN effect, influences in three interlinked, but distinguished, ways: a) as a policy-agenda-setting agent; b) an impediment to the achievement of desired policy goals, and c) an accelerant to policy decision making (Bøe-Hansen 2012, 145). Adding on the Al Jazeera effect[41] we include social media as a power factor, much with the same modes of influence as the CNN factor. Media, information and propaganda[42] is therefore key tactics to secure political say and position (Nissen 2013, 74). This process is called "the battle of the narratives". It rests on the idea that new wars include battlefields in the physical, moral and cognitive dimension. By combining ethos (trust/ credibility), pathos (emotions) and logos (facts)[43] (Casebeer and Russel 2005, 12), narratives create perception, which again found legitimacy and public support (Nissen 2013, 79–80). By writing the conflict narrative one can form the "why"; determining if one are a terrorist or freedom fighter, thief or Robin Hood, just or despotic. Both traditional and new media (like social media and websites) play a central role in this "battle of the narrative". Here combatants can foster support and promote specific perceptions and behaviors. Increasingly non-state actors also engage in this behavior. Fighting for public support and legitimacy can be a matter of survival, by swaying political decision-making in both states and international organizations (Nissen 2013, 74).

[40] A strategic narrative has also been described as a "…system of stories that share common themes, forms, events, and participants, and create expectations for how those elements can be assembled to satisfy a desire that is rooted on conflict"(Quoted from Nissen 2013, 73)

[41] Defined as "the suspension of traditional political connections that have brought identity and structure to global politics by the connectivity of new media, a rewiring of the world's neutral system" (Bøe-Hansen, 2012:145).

[42] Propaganda can be described as "a process of persuasion which utilizes any available means (media) to persuade people (target audiences) to think and/or behave in a manner desired by the source in order to benefit the interests of that source, either directly or indirectly" (Quote from Nissen 2013, 76).

[43] This Aristotelian model was first presented by Thomas Coakley in his paper on the Peruvian counterterrorism (Casebeer and Russel 2005, 12)

The softer version of war

The ultimate goal of the non-state actors is to undermine the opposition to the extent that it can claim results it would be denied by strength alone. In this thesis, this strategy will be referred to as subversion. Subversion can be understood as a deliberate attempt to undermine the trustworthiness and legitimacy of the established ruler (Rid 2013, 116). The ultimate goal is to overthrow the authority, but subversions can also have a lesser goal. The greater focus is to undermine social bonds, beliefs and trust necessary to maintain any organized collective. Not necessarily violent, subversion has historically manifested as ridicule, sabotage and protests to erode the power and repressive potential of a perceived illegitimate leader[44]. Hence, violence is not a mandatory participating factor as subversion relates to the current trend of "fighting for hearts and minds"[45](Rid 2013, 120). Soft war aims to alter the soft power balance, thus targets the relative influential power conflicting parties have on each other. When occurring in cyberspace, this form of behavior is quite similar to what Arquilla and Ronfeldt named "netwars" [46], but in this thesis the form of behavior relates to a conflictual form of behavior complementary to a real world conflict instead of the low intensity "kulturkampf[47]" described by Arquilla and Ronfeldt(Langø 2013a, 13). An understanding of what soft wars in cyberspace entail can thus be described as:

> To disrupt, damage, or modify what a target population "knows" or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may include public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote a dissident or opposition movements across computer networks (Langø 2013a, 13).

When discussing soft power, the weapons are tactics of propaganda and "selling the best story". "Soft cyberwar" is understood as the exploitation of the power and reach of the

[44] As seen during occupations, in repressive regimes, and by political opponents, who all aim to paint the other as incompetent etc.
[45] Insurgencies and revolutions are thus only the most dramatic forms of subversion (Rid 2013, 120)
[46] Arquilla and Ronfeldt define netwars as: Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt or damage what a target population knows or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may involve diplomacy, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movements across computer networks"(Arquilla and Ronfeldt 1995).
[47] The authors described netwars as: "distinct from cyberwar by being "normally about low-intensity conflict (LIC) and operations other than war (OOTW—a broader concept than LIC that includes peacekeeping and humanitarian relief operations). Given both its form (asymmetrical, non-hierarchical, and probably non-violent) and function (societal change), netwar can be seen as a hypothetical continuation of traditional Kulturkampf" (Langø 2013a, 13)

Internet (Geers 2011, 95) causing confrontation as part of a larger "battle of narratives". The founding belief is that new wars are not limited to the physical dimension, but also in the cognitive and moral spheres (Nissen 2013, 79–80). The approach places the population in the center, primarily fighting the opposition for the peoples' "hearts and minds" (Findley and Young 2007, 378). Beyond an audience, insurgents require the population for supplies and protection. The people therefore become the "center of gravity", described by Mao as "the fish and the water" (Findley and Young 2007, 383). They depend on the support of the civilian population, which must be secured by either their fear or their love. Soft wars thus target the population ("the sea") directly, and aim to build a supportive environment for the goals of a movement. Influencing perceptions can in turn affect the outcome[48]. By consequence the generation, management and potential manipulation of information is a source of power, again fitting nicely into the framework of "the battle of narratives" and psychological warfare. As the case study will reflect, the non-state actors discussed also take aggressive means of subversion to use; manipulation and hacking to strengthen the position of their perception of the conflict. As the social reality constructs how we understand ourselves, and others, shaping it may determine conflict (O´Hagan 2013, 561). In sum, narratives can fundamentally alter how we organize our mental understanding of the world (Casebeer and Russel 2005, 6). According to Sir Rupert Smith, new wars are characterized by the fact that "information, not firepower, is the currency of the new wars amongst the people"(Bøe-Hansen 2012, 145).

Information warfare consists of three pillars: a) attracting attention; b) raising emotions and feelings; and c) offering solutions to the crisis (Maliukevičius 2006, 137). Information warfare can, therefore, be understood as altering the context in which an agent receives information, either by manipulation of the actual information or its flow, by group pressure, or by propaganda (Bradsbury 2013, 15). Using information as a weapon therefore entails eliminating, distorting or stealing information for the purpose of obtaining necessary data after penetrating the security system (Applegate 2011, 19); blocking of access to information by its legitimate users (Applegate 2011, 19); information collection, storage, and dissemination can be compromised (Hutchinson and Warren 2001, 1); and lastly change the context to alter the interpretation of data (Hutchinson and Warren 2001, 1). Selective

[48] Hezbollah's actions in 2006 (vs. Israel) demonstrate the disruptive effect of well-executed information warfare. The militant group was outclassed in terms of military warfare, but used information warfare and political will to influence its outcome (quote Bradsbury 2013, 16).

information is presented, only referring to favorable facts. Additionally psychological pressure is added by painting a sense of urgency, hence disabling additional information gathering or rational reflection (Maliukevičius 2006, 138). It targets emotions and impulses to form behavior, not rationality. Consequently the sender attempts to shape the recipients' perceptions. It aims to create dissonance and disturbance in the public space, thus overshadowing alternative communications. Propaganda and information operations[49] also seeks to direct action by either agitate or pacify the recipient, or immunize them to alternative narratives (Bøe-Hansen 2010, 15).

> The basic tenets of information warfare are no different now than they were 100 years ago. The use of propaganda and the 'spinning' of messages are and always have been powerful weapons (Bradsbury 2013).

A clear understanding of what it entails is "a process of persuasion which utilizes any available means (media) to persuade people (target audiences) to think and/or behave in a manner desired by the source in order to benefit the interests of that source, either directly or indirectly" (Nissen 2013, 76). It can further be divided into "white" communication where the message is truthful and the sender is disclosed, "black" communication where the sender is fake/ unknown and the message seeks to deceit the recipient, and "gray" which reflects the middle ground between the two (Bøe-Hansen 2010, 15). All are founded in the four rules of thumb for mobilization during conflict situations; a) present a threat, b) report abuse and attacks, c) present the opposition as inhumane or unwilling to negotiate, and d) leave only military action as a viable option[50] (Nissen 2013, 76). Nissen describes the competing narratives' similarities as:

> Overarching narrative of their respective legitimate right to either uphold law and order against foreign-supported criminal groups or the rebels' right to defend themselves against an oppressive regime, they both produce and project stories and events that support these stories containing the elements of the continued threat (..) of the inhumane behavior of the other party (2013, 77).

[49] In NATO, information operations provide advice and coordination of military information to relevant parties. It has five key areas of operation: Psychological operations (PSYOPS), military misdirection, operational security, electronic warfare and network operations (Bøe-Hansen 2010, 18).
[50] All these trends are seen today in Syria, especially in social media.

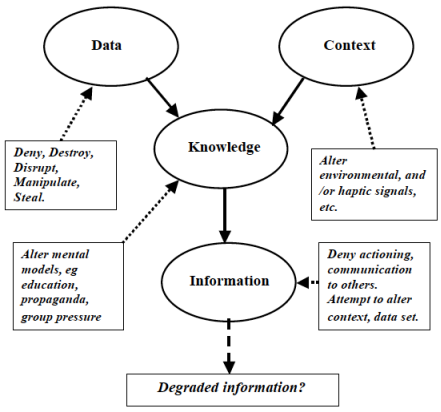

Figure 1: The tactics of information warfare (from Hutchinson and Warren 2001, 2)

Information, due to the spread of information and communication technology (ICT), is more important than ever. Though highlighted as early as Sun Tzu *Art of War*, it has diversified and increased since the 1990s (Cavelty 2013, 363). Uncertainty also forms a large part of Clausewitz's "Fog of War" (Lewis 2010, 4). Cyber attacks introduce a new dimension in the ability to create uncertainty and confusion among the opposition. This in turn slows decision-making, increases caution, and increase the probability of error. Cyber intrusions can thus degrade morale and the will to resist (Lewis 2010, 5), showing similarities to traditional guerrilla warfare in the physical world. It also becomes a way to humiliate the adversary and disrupt the opponent's conflict strategy. Cyberspace, due to the reach and low barrier of entry, also creates a new reality for the manipulation of information and presenting competing narratives. As seen in traditional conflicts, parties will use several mediums to present their version of events to the public. As computers, smart phones and the Internet become more available, the number of agents increases. Anyone may be a journalist, and in a conflict situation verification is complicated. So the separation between white, gray and black propaganda becomes harder. The Internet acts as a "force multiplier" (Goodman, Kirk, and Kirk 2007), facilitating large audiences and effects without the demand of more attackers. It provides a global forum in which actors can disseminate their propaganda. Additionally the scale of the domain makes any statement harder to refute. It has also become a mouthpiece to present threats, victories and accusations. These are often redistributed by the media and thus multiplying the audience and effects. As the technology behind this domain is little known, cyber fears may have unwarranted consequences and attention[51].

[51] As seen by the described cyberwar debate and the fears of a few, non-state individuals' ability to cripple a nations' infrastructure.

Methodology

The following chapter will outline the methodological choices made in this thesis and explain how the conclusions came about. This work utilizes the case study method, a well-known tool in political science, and therefore will not evaluate this unless relevant for the actual work undertaken here. It will instead focus on the strengths and weaknesses in this research project.

There are some methodological challenges in this project, mostly relating to the fact that little previous research is done. Firstly, most literature relates to inter-state conflict, while this work researches the combating non-state actors in an intra-state setting. Secondly, several methodological challenges plague the current cyber conflict literature: great disagreement relating to key terms and definitions; strong wording relating to the potential consequences and reach of cyber activities with malicious intent[52]; and a strict division between the literature focused on the technological issues and the strategic issues[53] (Mulvenon and Rattray 2012a, x). As a result, the thesis must balance various understandings, "languages" and methodological tools. Thirdly, the thesis combines insights from different fields like political science, political psychology, conflict studies, technological studies and media studies.

Research question and key assumptions

Any research project is founded in a specific topic and corresponding research question. As seen in the previous chapter, this thesis focuses on why and how non-state actors use cyberspace as a part of their strategy in a conflict situation. The research question becomes: *"Why and how do non-state actors use cyberspace in modern conflict?"*

To answer this question, certain assumptions are made. These are specific sub-questions that together build a train of arguments. This allows us to test the assumptions underpinning our research question. Firstly, non-state actors use cyberspace as part of their conflict strategy.

[52] Here I am referring to the writings of for example Arquilla and Ronfeldt (1993), or Lewis (2010),
[53] Intuitively this is unfortunate as it is unnatural to evaluate technical components without the necessary technical understanding, and limiting to only evaluate the technological security element without inclusion of the wider consequences. Thus both camps are diminished by the lack of cross-field cooperation.

Secondly, this thesis is founded in the belief that they use this domain not only as a mouthpiece but also as a strategic tool of subversion aimed at undermining their opponent. These "warriors" actively sabotage, persecute, and spy on each other and perceived supporters by hacking accounts, defacing websites and manipulating social media outlets. Pushing an agenda of subversion, it is a different and more conflictual form of cyber-interaction then analyzed before. They use this domain in conflict situations to exploit the potential for waging soft wars; a form of conflict participation where agendas and narratives compete. The third assumption is that they promote a strategic narrative and soft power through guerrilla tactics. The ways of real world conflicts are adapted to cyberspace, where the softer side of warfare seeks to damage the center of gravity in the opponent. This leads the conclusion that the "cyber warriors" seen in Syria is not a new phenomenon, simply the adaption of old strategies in a new domain. Lastly, the thesis operates under the assumption that the reach and effectiveness (measured in the level of attention and number of attacks) of the non-state actors depend on the level of organization and resources. These assumptions can be summarized in five points: (1) Non-state actors use cyberspace in conflicts; (2) Subversion is the ultimate goal of their actions in cyberspace; (3) This is done by spreading a strategic narrative and build soft power; (4) To reach their goal, they use guerrilla tactics; (5) The effectiveness is determined by level of organization and resources. The case study method is perfectly suited as it will give us deep insights to the subject and "are more useful for generating new hypothesizes, all other things being equal" (Gerring 2007, 38).

The case study

Gerring describes a case study as "a spatially determined phenomenon observed at a single point in time or over some period of time" and "the intensive study of a single case where the purpose of that study is – at least in part – to shed light on a larger class of cases" (2007, 19–20)[54]. King, Keohane, & Verba (1994) exemplifies; " a uniquely bounded phenomenon in a historical or geographical sense, such as the case of Munich, the Soviet invasion of Afghanistan, or the Watts riots " (Kaarbo and Beasley 1999, 372). We therefore see that a case study can be understood as the scrutiny of a certain object, not naturally distinguished from the surrounding process. Generalization is not the main desire, compared to statistical

[54] Ringdal (2007, 149) describes a case as "one or more units of analysis that are objects of scrutiny[54]". George and Bennett adds that it is "the detailed examination of an aspect of a historical episode to develop or test historical explanations that may be generalizable to other events" (2004, 5)[54], thus including time and the potential of generalization.

studies where the intention is finding the average effect on a wide range of cases. The case at hand is the non-state actors who operate in cyberspace as part of a conflict strategy in Syria between 2011 and April 2014.

The Syrian conflict itself and the analysis of cyberspace as a warfare domain are unproblematic as several excellent inquiries exits (see for example Carr 2011; or Rid 2013). In this thesis, the case study is the Syrian conflict's cybered aspects. As the Syrian Electronic Army, the most significant actor, was established in the fall of 2011 (SEA 2014) this is seen as an appropriate starting point of the research. The thesis is submitted in May 2014; thus the research must end at an appropriate time before this date. The end of primary data collection is therefore set to 01.04.2014. Though rather short time, this is deemed fitting both considering the scope of the thesis and the circumstances. Though the case study is Syria, certain limitations have also been done. Due to space considerations and available data, the actors researched are limited to the organized parties with enough attacks to reflect a strategy. Therefore individual actors responsible for single attacks are not included. In sum, the main object of research is therefore the pro-regime cyber units (exemplified by the Syrian Electronic Army) and anti-regime groups. The research object can be understood as "Syrian combatant non-state actors in cyberspace"[55]. As the anti-Assad opposition is not organized enough in cyberspace, it has not been possible to limit the research to two opposing "cyber-guerillas". The firmest conclusions are related to the actions of SEA, as the majority of the empirical data relates to this group.

This thesis will explore both a new phenomenon (cyber warfare) in a traditional framework (intra-state conflict), and evaluate if old tactics (information and psychological guerrilla warfare) can be beneficial in cyberspace as well. The inspirational fields are well documented, though few similar research projects are undertaken. The case study is therefore understood as a hypothesis generating case study (Levy 2008; Lijphart 1971). There are two reasons for this: a) the aim of this research is closer acquaintance with a new phenomenon, and b) the empirical record is little and conclusions relating to a broad specter of events are therefore neither possible nor the goal. By combining insights from the several academic fields with primary data collection, this thesis can generate new insights into this ongoing

[55] Either cyber militias with clear links to governments or military actors in a inter-state context. Some similar studies on European groups have been conducted by Rain Ottis at the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) and by Scott Applegate for the US Army. Their work inspires and somewhat guides the primary data collection, though they both focus most of their work on state actors.

conflict. However, as little similar work can be used to measure the reliability, conclusions must be seen as indicative rather than conclusive.

Primary and secondary data collection

Case studies are excellent for exploring why something happened and how it came about, as it gives insight into motivations and events to an extent lost on the more quantitative methods. Due to the closeness to the data, the research method can examine new causal explanations, mechanisms, parameters and variables (Collier, 1999, in Levy 2008, 5)[56]. It also simplifies the inclusion of context and a deeper understanding (Bennet 2004, 34–37; Moses and Knutsen 2007, 54). The case study gives an advantage of insights to elements unfit for existing theories by questioning hypothesizes, parameters and established truths (Levy 2008, 5). It is therefore a method for generating new knowledge (Eisenhardt 1989, 85–86). Only by using the cause study can the nuances be captured, and the individual differences studied to the necessary degree.

> Case studies emphasis the contextual reality, and favor deep knowledge. However this may cost the width of the research project if favor of depth (Soy 1997).

The data collection is a combination of targeted literature search and a large collection of primary data on attacks completed during the Syrian conflict[57]. One of the main contributions of this work is therefore an extensive empirical record of cyber attacks during the Syrian conflict[58]. All attacks meeting the criteria[59] are included in the attempt to provide as unbiased review as possible. This is presented in the appendix, and forms the basis for the evaluation done in the analysis though the findings of others are included to increase the legitimacy of the research. The primary data for this thesis will to a great extent depend on what can be labeled "contemporary sources"; it has not been submitted to peer review and are for example blogs, twitter feeds, YouTube videos and Facebook statuses. The trustworthiness of the

[56] "Given their close proximity to and familiarity with the data, case study analysts are well positioned to suggest additional explanatory and contextual variables, causal mechanisms, interaction effects, and scope conditions"
[57] Case study data can be collected from historical sources, registered data, interviews, fieldwork and surveys (Ringdal 2007, 150).
[58] Though the majority of the available data is related to SEA, but the works of international actors in collaboration with the opposition will be included. As the opposition lacks a specific cyber-army similar to SEA, ignoring the works of Anonymous and #OpSyria would therefore limit the research to SEA as an organized actor and some short-term groups of opposition individuals.
[59] Non-state actors, of a certain level of organization, presenting a strategy over time.

sources therefore can and should be questioned[60]. However, any individual hack is given little authority if not confirmed by the victim or another credible source. Any claim of hacks is only given credence if verified by secondary, independent sources like media articles or seen by the author herself. Attacks that are not confirmed by several source or peer-reviewed by fellow academics are excluded to secure the quality of the research. The thesis therefore depends on a strict criterion of verification and restrictive interpretation, which possibly limits the amount of data collected[61]. There has also been a comprehensive literature review to complement primary data and conclusions. Peer reviewed journals are used for the theoretical foundation and the empirical records[62], as reflected in the bibliography. Reports from reputable institutions are also used as collaboration of attacks to the extent possible.

There are challenges relating to categorization. Awareness of the gray area between hacking (defacement, alterations of platforms and websites, use of code) versus social media exploitation[63] is therefore necessary. These challenges additionally relate to the clandestine nature of the research object. Though the groups in question often boast of their actions, their links and dependence on formal organizations are kept secret. There are insecurities relating to the independence of the groups, their sizes, and ownership of hacks. In the primary data collection this challenge is redeemed by restrictive classification, based on the type of attack. The relative importance of an attack is based in the importance of the victim, as it is expected that a news agency have a greater security apparatus then civilians. The former victim thus requires more resources and expertise to successful hack. Another issue concerning primary data collection is the bias caused by the dependence on western sources. The Syrian Electronic Army has made a name for itself in certain milieus due to its attacks on several international news agencies. No other Syrian cyber militias are discussed at that level in either mainstream media or academic journals. The author reads Norwegian, English, Spanish and some French but is not competent in Arabic. Unfortunately that means that the relevant sources in this language are excluded. As social media updates by some groups are only written in Arabic, these groups have surely not attracted the deserved attention. It is likely that the Syrian opposition has higher representation in this group than the pro-regime attacks as the SEA publishes in both Arabic and English. However, all secondary sources

[60] For example, it is easy for an individual to manipulate pictures proving a hack of a website
[61] This research also seeks to interpret the trends of the hacks, not independent events.
[62] Academic reports evaluating cybered events in Syria as well as news reports are consequently given more credence than self-reported attacks or events only referred in blogs etc.
[63] When a profile is stolen by traditional social engineering, not spyware, and used for impersonations online.

support the view that the opposition lacks the necessary organization, expertise and authority in cyberspace. Translated material is also included when relevant and verified, both from social media and other researchers.

Strengths and weaknesses

Bennett (2004, 39–43) and Gerring (2007) identifies certain trade-offs when choosing case study as a research tool: a) Case selection bias (choosing the research object based on the dependent variable) vs. Confirmation bias, b) difficulties identifying the dominant cause, c) potential for generalizing results, d) risk of non-independent cases[64] (Bennet 2004, 39–43). In sum the case study is overall a better method when a) data is descriptive instead of causal, b) deep insights are prioritized over the broader scope, c) internal validity is prioritized over external, d) the research seeks insight to causal mechanisms, d) the research is exploratory, e) there are few potential cases (Gerring 2004, 352). As seen in Table 2, these trade-offs correspond greatly with the research goal of this thesis.

Table 2: Trade-offs case study vs. statistical analysis (Gerring 2007, 38)

	Case study	Statistic analysis
Research goal	*Hypothesis generating*	*Hypothesis testing*
Prioritized validity type	*Internal validity*	*External validity*
Causal insight	*Mechanisms*	*Effects*
Empirical focus	*Deep*	*Broad*
Population	*Heterogenic*	*Homogeneous*
Source material	*"Thick", diverse data*	*"Thin", standardized data*

Any research project is evaluated by its methodological quality; in which the key components are construct validity, internal validity, external validity and reliability. The level of internal validity describes to what extent the causal path is correctly identified (Cook and Cambell 1979).The case study enjoys a strong internal validity due to the deep insights and closeness to the data, which is true in this case as well. The author has followed these groups for over a

[64] Galton's problem: "correlations between social institutions might not only arise under pressure of functional exigencies (that is, through processes operating within societies), but also as an effect of cultural diffusion between societies (Scott and Marshall, 2012).

year, and studied their doings in detail over a limited period of time. Construct validity entails that the correct measurements have been used to study the concepts, while external validity describes to what extent the results can be transferred beyond the immediate case(s). Both these validities are of lesser importance in this work, as it does not exist any established measurements due to the newness of the phenomenon. Secondly it does not seek to transfer the results, only to understand the research object and possibly develop a formula for further exploration of non-state actors in cyberspace. The external validity is therefore less relevant for this case as the thesis hopes to explore a sub-field rather then generalize across a number of empirical cases. It is also rather short empirical record of conflicts that include the cybered element, and they greatly vary to what extent[65]. As the advantages of the case study method in general and the goal of this case study strongly correspond, the case study method is deemed the most appropriate for this study. As seen in the Table 2 *Trade-offs Case study vs. Statistic analysis,* the gains by far outweighs the flaws.

The reliability describes the accuracy of the study, and by consequence if it can be replicated (Soy 1997). This is always complicated with case studies as they include a wide range of variables and context. The same is true in this case, but the appendix provides a detailed description of all the attacks included in the analysis, thus facilitating replication. Lastly, causality may be complicated in the social sciences as few phenomena have a clear construct. This is defined by Gerring as ”the core, or minimal, definition of causation held implicitly within the social sciences is that a cause raises the probability of an event occurring.” (2005, 167). This is obviously complicated in this case study as it is almost impossible to isolate events and determine if Y follows X. However, as this case study does not look at effects, causality is of less relevance. The case study is more applicable to the research into the causal mechanism (what causes what) than the causal effects (Gerring 2007, 53–56), as is the target of this investigation. This work has the purpose to establishing that something happens, not in what order. Regardless, it is important to remember that this may lessen the generalizability of the work (Gerring 2007, 44), as they deep insights into a specific phenomenon lessens the potential for broad conclusions applicable to a wide number of cases.

The aim of the method is to understand “the greater picture”. However, this causes a lack of control and possibility for replication. The number of variables is rather great, especially

[65] Examples are the Middle East conflict, Hezbollah operations against Israel, Georgia –Russia conflict, and Estonia- Russia. All these conflicts had some cybered aspects, but great differences in execution and goals.

when exploring a single case. Regardless this is not seen as a great shortcoming as this research does not seek to develop a grand theory. This project only seeks to explore a potential framework for evaluating a new phenomenon in a specific context, possibly indicating a new use of old insights. The generalizability and replication are thus of lesser importance, as the research is hypothesis generating. However, if findings are to be transferred to other similar cases, the mentioned methodological challenges must be addressed. In this research, the case is chosen due to the wish to explore the present dependent variable, and thus random sampling has never been an issue (Bennet 2004, 19–20).

In sum, Syria is not an easy case to evaluate. Firstly the conflict is ongoing and thus much of the data is contemporary, disputed, and influenced by the chaotic situation in ongoing civil war. Though important to keep in mind when evaluating the conclusions of this thesis, Syria is also an important case much due to the same reasons. The Syrian case is somewhat unique as it is related to the Arab Spring, but show many different traits in its horrors, length and lack of unified opposition. It is also the first cyber conflict of its kind. Though some events mirror the same tendencies (especially Estonia 2007 and Georgia 2008[66]), this is the first internationalized cyber conflict where both parties involve non-state actors in an organized manner resembling a "cyber guerilla"[67]. Also, both parties are organized in cyberspace and are accused of using this domain as a battlefield for psychological and information warfare. We see tendencies to strategies where both traditional and social media are used in a coordinated manner to intimidate enemies, legitimize own actions, and sell narratives. Additionally hackers are playing a vital role in this battle, thus going beyond the scope of "Facebook revolutions[68]". Lastly, it is also the first where an "international force" (Telecomix and Anonymous' #OpSyria) has assisted local cyber-actors in a coordinated, global effort. To fully understand the role of the non-state actors in cybered conflicts, Syria is the natural choice.

[66] In these cases non-state actors were highly involved in the electronic elements of the conflict, especially by Russian sympathizers. There are several analyzes of these conflicts, especially by the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE).
[67] Representatives from both sides of the conflict has explicitly mentioned cyberspace as part of the conflict strategy, while both Estonian and Georgian conflict was dominated by individual citizens falling clearly within the category of "patriot hackers" as discussed later on.
[68] Here private citizens use social media to inform and coordinate action, but hacking skills are not used to manipulate, alter, influence or prevent behavior.

The Syrian question: the how and the why

In Syria, there are three non-state actor parties to the cybered conflict. Firstly, there are the regime supporters, represented by the Syrian Electronic Army. This group has to date reflected the highest level of organization and sophistication. Secondly there are the anti-regime groups, which operate as a loose collective linked with various rebel groups. Lastly, there is the international element, reflected in the involvement of global hacker communities like Anonymous and Telecomix. In this thesis, the international element will only be included when they aid anti-regime groups, and these are therefore analyzed together.

The case study, and Shehabat (2012), finds that both sides of the conflict pursue strategies of cybered information and psychological warfare. Aided by social media and cyber attacks, they spread their narrative, monitor each other, and undertake disinformation campaigns by means of propaganda and hacking. The Syrian conflict is also unique as it is the first where cyberspace is used extensively by both sides of the conflict (Shehabat 2012), and both go to extraordinary lengths to sabotage, disrupt and destroy the other (Salhani 2013).

This case study consists of several sections. First the technological situation in Syria will be outlined to facilitate understanding of the environment in which the actors operate. Secondly, the main actors are introduced. Thirdly, an overview of the trends in Syrian cyber attacks between 2011-2014 is provided, divided into three sub sections. Then a discussion on the assumptions and findings is presented in the sub-chapter "the Syrian cyber battle". Before the final remarks, we conclude by taking a closer look at to what extent the cybered aspect of the Syrian cyber conflict qualify as a soft war. The course of the conflict will not be described unless it is relevant to the technological aspects of the conflict, as several excellent overviews already exits[69] and this work operates under space limitations.

[69] For a brief introduction, see for example overviews produced by The Huffington Post http://www.huffingtonpost.com/johncurran/syria-explained_b_4059238.html or the BBC http://www.bbc.com/news/world-middle-east-26116868.

Syria and cyberspace

Before acquainting ourselves with the main actors in the Syrian cyber conflict, we need to describe the state of Syrian cyberspace as this provides the framework for the actors to operate within.

Looking back, we can identify some key steps in the development of technology and media in Syria. The development of Information and Communication Technology (ICT) can be argued to correspond with the power of the Assad regime, which has a long tradition for information manipulation. Starting with the 1963 coup d'état, the media became a tool of government propaganda and control (Baiazy 2012, 1), and media freedom degraded rapidly. The state controlled newspapers, books, radio and television broadcasts, and advertising. After 1974, the Syrian media's main task was additionally to promote the personal cult of President Hafez al-Assad (Baiazy 2012, 1), and critique of the president or the ruling elite is to date forbidden. However, from the 1990s the Arab world experienced a media revolution as satellite television and the Internet was introduced to the region. For a time the possibility of state control was limited, and a vibrant social media environment emerged. As new technology was introduced, new voices were heard and challenged the informational hegemony of the regime. A process of opening started, but Syria is a long way from a technologically developed society with free media. Despite rapid growth in infrastructure and use, there is still a low level of penetration, lack of human capital and little ICT expertise (Khamis 2013, 1). Lastly, the current phase started in 2011. A media reform package was tailored to meet the demands of protesters, when decree 108/2011 defined the media as free and independent. However freedom is still limited by the constitution and national security considerations[70]. The decree also prohibits any information that "weakens national unity" or "harms state's symbols". In reality this wordings can be interpreted to entail a wide range of information, and media freedom is at best established on paper (Baiazy 2012, 1–2).

Telecommunications in Syria is highly regulated, and infrastructure is owned by the state through the state-owned Syrian Telecommunication Establishment (STE). The Syrian Informatics Society, with the president patrons, monopolizes the Internet and supervise all private Internet Service Providers (ISP) (Baiazy 2012, 15). The government dominates the

[70] Including any content harming religion, initiating crimes, violence, terrorism, hatred and racism, and any news relating to the armed forces (Baiazy 2012, 1–2).

market, creating one of the most controlled in the region. The regime and supportive businessmen have controlled the media infrastructure for decades, thus silencing opposition and securing international legitimacy (Khamis, Gold, and Vaughn 2012). Monopolies are protected to control public opinion, and great investments are made in sophisticated cyber surveillance (Baiazy 2012, 15). Lastly, the Syrian conflict has seen several disruptions of cellular and Internet communications[71] (Bradsbury 2013, 14) to prevent citizen journalism and communications between rebel fighters (Freedom House 2013). However, the regime is cleverly sensitive to not enrage the unaligned population by long-term blackouts as in Egypt and Tunisia. SEA also blames the insurgents whenever ICT malfunction, thus sharing the blame and challenging the narrative of the regime as oppressive. The case study indicate that the Syrian regime and its supporters studied the Arab Spring, and make sure to avoid making the same mistakes as the now toppled regimes in neighboring countries.

Simultaneously as control of cyberspace is growing, Syria, as well as much of the Middle East, has experienced a massive surge in both infrastructure and users over the last decades. Syrians online has grown from 30 000 to 5 million (Reporters without Borders 2013) in just ten years[72], and social media has exploded[73]. Regardless, it still influences only a limited percentile of the Syrian people (Baiazy 2012, 12; CIA Factbook n.d.) consisting of almost 18 million individuals (CIA Factbook n.d.). In comparison, there are 12.9 million (2012) mobile phones in the country[74]. Facebook, Twitter, Skype and Yahoo Messenger all broadcasted news and information, both genuine and manipulated. To prevent the reach of these devices, the Assad regime even banned IPhones at one point (Shehabat 2012). Today the Assad regime has also increased online surveillance and blocked Internet access on various occasion. However satellite telephones, international SIM card and proxy modems limits the effectiveness of the limitations.

[71] For example in August 2012, services were cut in the second largest city, Aleppo. Less than two weeks earlier the whole of Syria was disconnected from the Internet for 40 minutes (Bradsbury 2013, 17)
[72] 2000 to 2010
[73] ”From December 2008 to March 2011, the number of Twitter users in the Middle East and North Africa exploded, from 1,335 to nearly 1.2 million. While the UAE leads the region in numbers and user activity, activity is growing fastest in Lebanon, Syria, and Jordan” (Quote from Baiazy 2012, 11)
[74] By far surpassing the use of fixed telephone lines with 4.425 million (2012) users (CIA Factbook n.d.).

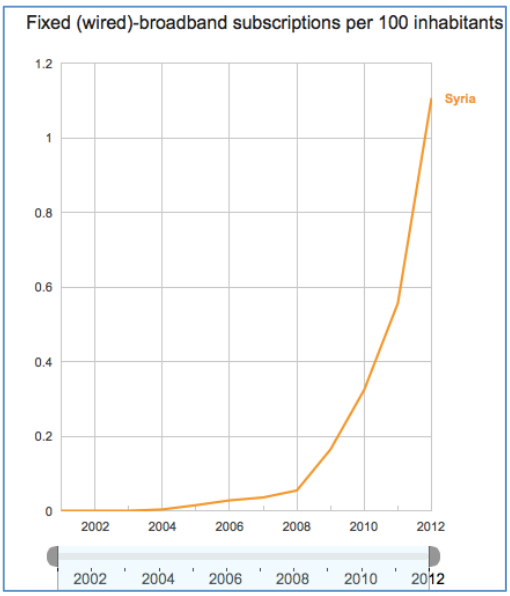

Figure 2: Fixed broadband subscription per 100 inhabitants, Syria (International Telecommunication Union 2014)

From 2000 to 2012 internet users in Syria grew from 0.2% of the population to 22.5%, but still only 35% of households (2010) have internet access (International Telecommunication Union 2013). Now security officials require picture ID and registration at Internet cafés, to prevent acts by "destabilizing elements"(Baiazy 2012, 14). In February 2011, social media sites like Facebook, YouTube and Twitter was again available in Syria after three years blockade (Baiazy 2012). Today about 10 000 people join Facebook in Syria every month (Baiazy 2012, 5), making it one of the most important channels for news, information and interaction with others. The reopening happened after a Syrian Revolution page appeared on Facebook and events escalated in Tunisia and Egypt. However, activists claim that it was done only to facilitate surveillance, and push rebels to abandon anti-detection software (Baiazy 2012, 18). Since the start of the revolts in 2011, the regime has also several times closed media offices, limited internet access and prevented journalists' investigations (Baiazy 2012, 7).

Reporters without Borders categorize the media system in Syria as authoritarian (2013), where the regime's needs for legitimacy and stability dictate communication development. Freedom House concurs and scores Syria 85 point on a scale where 100 represent total government control online (Freedom House 2013). The media is controlled by financing, licensing and legal means. It in turn protects the regime and circulates the policies of the

government. The revolts have decentralized the media, though censorship is broad and harsh punishments common. Bloggers and users of social media still risk intimidation, arrest and torture (Khamis, Gold, and Vaughn 2012). Some reports even indicate that activists are beaten until they reveal their social media login credentials. Regime agents then use stolen profiles to spread information under false persona. Information found is also used as proof of anti-establishment behavior (Deibert 2013). People, therefore, share passwords with trusted friends so these can delete any incriminating online critiques if they disappear (Preston 2011). In all, the level of surveillance and fear of harsh punishments pacify the citizenry. According to Freedom House,

> In an environment of extreme violence and arbitrary "red lines," self-censorship is widespread. Most Syrian users are careful not only to avoid such sensitive topics when writing online, but also to avoid visiting blocked websites (Freedom House 2013).

Together this makes Syria is one of the least developed markets in the Middle East, with a long tradition of blocking foreign websites and censorship. The combination of low levels of human capital and development, but massive surge in users, resembles the rest of the Middle East affected by the Arab Spring. However, as the case study will show, the actors in Syria face a different reality than seen in Tunisia and Egypt. But before exploring the responses to their cyber environment, we must acquaint ourselves with the main players.

The main players

The following section is divided into two parts, one for the each of the parties in the Syrian conflict[75]. It will outline who they are, and how they are organized. After this introduction, the thesis will move on to the main part of the case study, which evaluates what actions the players have undertaken.

The pro-regime faction: The Syrian Electronic Army

The most referenced actor is by far the Syrian Electronic Army (SEA), which emerged in 2011. SEA declare on their 2014 website (SEA.sy) that they are independent citizens, who formed the organization in response to:

> The Arab media and Western media's bias in favor of terrorist groups that have killed civilians and the Syrian Arab Army, and destroyed private and public property (SEA 2014)

They go on to describe their vision as:

> We hope the experience of the Syrian Electronic Army to become taught in the future for the people who refuse to kneel to the West and that our experience becomes an approach for the coming generations to walk in our footsteps. We are a peaceful resistance because we want only to carry the weapon of knowledge (SEA 2014).

Their vision and purpose have remained steadfast over the course of the conflict. However, this study shows that the group has evolved over the last couple of years. Perlroth (2013) finds the same tendencies, and concludes that different individuals make up the SEA today then in the beginning. In 2011, there was a clearly defined hierarchy with a leadership structure, media representatives, technical experts[76] and volunteers (Perlroth 2013). The group also started in 2011 what can be understood as a virtual academy, called "The Syrian Hacker School" to recruit and train sympathizers in the use of DoS, computer infiltration and electronic surveillance (Noman 2011a, 13). Today though, the group most likely consist of members categorized as civilians with technical training or professional hackers (Fisher and Keller 2011). Resembling Anonymous, a loose networking structure is lead by a dozen members known under aliases like "the Shadow" and "Th3Pr0". The SEA spokesman,

[75] As stated before, international actors will only be evaluated together with domestic cyber actors. This limits the number of parties from three to two, though the international element is still included in the analysis.
[76] Most likely from the Syrian Computer Society.

Th3Pr0, regardless claims that the group consists of thousands of members (Assir 2013) who function on a volunteer basis. But there are some indications that the groups is now reverting back to a firmer organization, as the new website indicate at least attempts to coordinate and define leadership structures.

The relationship between SEA and the Assad-regime is disputed for several reasons. For one, reports indicate that the group passes on opposition's identity and location to the Syrian security forces. Also, the group is able to operate without any known interference from the regime, signaling at least tactical support (Noman 2011a). Additionally the original SEA website domain (Syrian-es.com) was registered to the Syrian Computer Society on May 5th 2011, an organization founded by Bassel al-Assad77 and later headed by President Bashar al-Assad (Fisher and Keller 2011). President Assad's cousin Rami Makhlouf also supposedly pay members between $500-1000 per month, and provide training in both Syria and Dubai with support from Russia (Harding and Arthur 2013). Lastly, President Assad also referenced the group in a 2011 speech, stating that:

> The army consists of the brothers of every Syrian citizen, and the army always stands for honor and dignity. Young people have an important role to play at this stage, because they have proven themselves to be an active power. There is the electronic army which has been a real army in virtual reality (Quoted in Fisher and Keller 2011).

SEA, however, vigorously refutes any claims of sponsorship, but voice strong support of Assad and his regime. Their spokesperson,"Th3Pr0", stated in an interview 30.04.2013 that "If the President lose then Syrian and the Syrian people will lose, but Syria will not lose... the right never lose" (Stalinsky and Sosnow 2013). In sum, it is uncertain whether the SEA is contracted, integrated or simply likeminded to the regime. It is regardless clear that both the SEA and the regime benefit form the current ambiguity as the regime cannot be held accountable for SEA's actions, for example when the group attacks foreign media websites. The regime run less risk of other countries waging high sophistication cyber attacks as long as the proxy relationship remains. SEA also profits as it may operate with tactical support, but without constraints. It is therefore likely that the current marriage will continue.

According to the group, SEA's work is built around three axes: Facebook, Twitter and cyber attacks (SEA 2014). It is therefore impossible to ignore their social media strategy, though

[77] Bassel al-Assad was the eldest son of former president Hafez al-Assad, and was intended for the presidency before he died in a car accident in 1994. His brother Bashar al-Assad therefore succeeded their father as president of Syria in 2000.

this is not the main focus of this thesis unless it relates to unauthorized use, access or other forms of hacks. SEA profiles on sites like Facebook, Twitter[78], YouTube, Instagram, GooglePlus and Pinterest present "proof" of the rebels as foreign agents, vandals and refute any dwindling support for the government. These sites are therefore targeted by domestic and international opposition forces, and have been deleted repeatedly due to violations of the services' Terms of Use agreements. These sites are regardless quite popular, the latest Facebook page had for example 4686 likes after only five days[79]. Several reports indicate that social media also is used to spread spyware, build narrative, and as a medium for information warfare. Their own statements also support the analytic format of this thesis, as the SEA describes their reasoning for hacks as follows:

> (….) due to the lack of ways to deliver a picture of events for what they are in Syria and the bias of the media coverage of the Syrian opposition, which the whole fabricated and unbalanced, we may have a number of times to break through news sites worldwide to put the news of our country as they are and explain to our young people, Syrian believer, and do not deny many of the times that we hacked e-mails and pages for individuals, institutions and media organizations and the opposition of hostile policy of the Syrian Arab republic and we post them to the public to understand the world the size of the plot hatched against our country from the financing, arming and publishing false news (SEA 2014).

We now have a clear understanding of the pro-regime fraction, represented by the SEA, and move onto the opposition's less organized approach. The groups' actions are described in detail later.

78 Both their Facebook page and Twitter account has been deleted repeatedly, SEA claims 239 and 15 times respectively (SEA 2014).

79 Unlike its former Facebook pages where posts was made in both English and Arabic, and the current website, this Facebook page only posts in Arabic. See the 292nd Facebook page at: https://www.facebook.com/SEA.292. The current was established April 4th 2014, and it is possible that SEA now only posts in Arabic to avoid detection by Facebook administrators that have shut down former sites. However, the SEA twitter account continuously links to the Facebook page to entice followers in both platforms.

The anti-regime faction

The anti- regime fractions focus their work on promoting the rebellious narrative, support moral of fighters, and discredit the regime (Shehabat 2012). The opposition has been operative in cyberspace since the start of the uprising (SECDEV Foundation 2013a), and in the beginning was clearly the winner in cyberspace. Today though, the opposition functions as a loose collective, lacking the force of a unified group. The groups vary in size and professionalism, but generally target government websites or computers. This research also indicates that rebel operations are either a single attack by one or few individuals (and therefore excluded from the empirical material), smaller groups with a limited number of attacks, or operations in cooperation with international actors. The empirical record also reflects the lack of a comprehensive strategy between the many groups, and lack of coordination. This will be further discussed later on.

Some of the main anti-regime actors in Syria, with some duration, are according to the SECDEV Foundation (2013a, 4):

- *The Chinese Army for Crushing Syrian Regime Shabiha*: created in September 2011, this group removes Facebook and YouTube channels of pro-regime groups. It has been quite successful in spamming social sites, and also uses mass reporting of violations to Terms and Conditions relating to hate speech and incitement to violence to force the sites to close certain pages or channels. It is the most persistent of the anti-regime hacker groups, and is based in Syria.
- *Hackers of the Syrian Revolution:* this group focuses their attacks on regime computer infrastructure. It appears to consist of only four individuals, but has successfully hacked computers at the Ministry of Oil and Mineral Resources, the Syrian General Security Department (GSD) and the state-owned Syrian Virtual University in 2013. The published internal memos from the GSD, including the names of 700 people sought by the regime. By help of social media platforms, the hackers also seek to expose and discredit individuals.
- *Jabhat Al Nusra Electronic Army*: the groups Facebook page has existed since the summer of 2013, and claims that the hackers are affiliated with the extremist militants of Jabhat Al Nusra[80]. There are some indications that the group operates out of Abu

[80] This is yet to be independently confirmed (SECDEV Foundation 2013a, 4)

> Dhabi and Damascus, and condemn Shiite religious orientation. To date the group has defaced the website of Addounia TV, a pro- Assad satellite channel, and claim to have gain access to computers and social profiles of pro-regime individuals. It also targets members of the pro-regime Shiite militia Abu Al Fadl Al Abbas, People's Committees, and the National Defense Forces.

SECDEV[81] finds that these are the main anti-regime actors, but the empirical record collected for this thesis does not reflect the same importance and their influence is therefore not evaluated as especially strong. As seen in the record of this thesis, the attacks by the anti-regime faction are rather dispersed, and few groups have completed multiple attacks.
Syria has a high level of mobile phone penetration, facilitating wide broadcast of videos (Shehabat 2012). Portraying the regime's actions, the Syrian Free Army has also established press offices called "Local Coordination Committees" (LCC) and Facebook groups which allows communication domestically and internationally (Shehabat 2012). They circumvent limitations by accessing servers in neighboring Turkey and Jordan, to avoid regime surveillance and detection (Khamis, Gold, and Vaughn 2012, 13). However, this is only possible in border towns, where networks have been established to collect firsthand testimonials of regime brutality within Syria (Shehabat 2012). Individuals located across the border then spread the news globally[82]. The most important channels for the opposition are Facebook and YouTube (SECDEV Foundation 2013a); mimicking protesters instead of the cyber force at least the pro-regime aspire to become. This is also probably why the SEA has targeted these sites with malware and spyware, ultimately giving associations to the self-censorship imposed in Orwell's novel "1984" and Gestapo's Germany.

Compared to the SEA, the Syrian opposition lacks a united organization with the same level of sophistication and holistic strategy as the SEA. There are several minor groups that seem unable to launch larger campaigns together. As in the real world, the opposition is hampered

[81] The Foundation is a Canadian-based, not-for-profit organization, whose work has been supported by the International Development Research Centre (IDRC), Freedom House, The Open Societies Foundation, the Global Peace and Security Fund (DFATD), the US Department of State's Bureau for Democracy, Rights and Labor, and the Montreal Institute for Genocide and Human Rights Studies. They have partnerships and projects in Latin America, the Middle East, the CIS, Sub-Saharan Africa, South East Asia, Western Europe and the United States. They are privy to information, resources and a time frame not available for this thesis- and their findings are therefore included though the empirical material does not reflect the claimed position.

[82] Obviously fact checks and journalistic integrity is then next to impossible, making manipulation easier though multiple sources are officially required (Khamis, Gold, and Vaughn 2012, 20).

by the multiple fractions and its' inability to cooperate. The regime's high capacity in surveillance, censorship and disruption of Internet access also complicates the establishment of a professionalized force within Syria. The pro-regime activists use Remote Administration Tools (RATs), phishing, DDoS attacks, defacement and malware to hamper the work of the rebels. Of low sophistication, these tools resemble low-level espionage and sabotage. However, it is a disturbance, and the surveillance capabilities may prevent supporters joining the cause. Less funded and coordinated, the anti-regime groups are also more vulnerable. Again this mirrors the realities of the physical conflict. The hostile environment limits the effectiveness of anti-regime hackers, the construction of a wide reaching narrative, and complicates the unification of cyber campaigns. Undependable electricity and Internet access hamper anti-regime hackers' efforts, human capital is lost as a consequence of the physical conflict, and the deterioration of the physical conflict has led supporters to focus their resources on military or humanitarian aid (Sumey 2013).

Therefore the cyber opposition has sought support abroad, both from hacker communities like Anonymous or Telecomix, and Islamist groups like Ahrar al Sham Technical Office and Jabhat Al Nusra Electronic Army (SECDEV Foundation 2013a, 3–4). These networks are international hacker communities with a flat organizational structure where individuals join for specific causes. Short-term they may have some impact and gain attention, but their loose organization and broad scope of attention damages the potential for continuity. Thus, cyber power of the opposition has fluctuated greatly during the Syrian conflict, mostly dependent on the amount of support from abroad. With help, the opposition has successfully completed several phishing campaigns and RAT operations to gain control of targeted computers. Typically, these belong to the Syrian government, pro-regime individuals or social media sites of pro-regime groups (SECDEV Foundation 2013a, 3–4).

In 2012 Anonymous declared its support to the rebellion and some subversive results were achieved. In November 2012 the alliance was reaffirmed as Anonymous declared war on Assad after he threatened Internet blackout in Syria (Bennett-Smith 2012). The group also launched the global effort #OpSyria[83]. However, few records of attacks are confirmed for this research, despite grand claims by Anonymous. But some attacks received widespread

[83] Anonomous stated that the operation had a twofold goal: "One: gather any and all media coming OUT of Syria and spread the info. And two: OFFENSIVE, we are going to take down EVERY Embassy in the world Assad has left, begining with his biggest and most powerful supporter nations."(Phelan 2012).

attention, especially Anonymous' breach of SEA's servers leading to the publication of members' identities and passwords (Boone 2013). The Syrian Free Army (SFA), in cooperation with Anonymous, also has had some success disrupting and embarrassing Assad and his followers by publishing private correspondence. The strategic effect is questionable, though the signal effect may be consequential as it damages the Assad cult developed over the last decades. According to the Washington based research project CSPRI, USA has also provided the anti-regime forces with some training in encryption, circumvention of firewalls, and securing communication (Sumey 2013). Additionally the New America Foundation provided the rebels with devices that will secure Internet access regardless of regime-implemented blackouts (Sumey 2013). Some defensive aids have been developed, like "panic-apps" that delete all information or present false screens on smartphones (Sumey 2013), but in comparison to the SEA the anti-regime forces are outnumbered and out-resourced. These international campaigns have some impact within Syria, but their domestic nature force less international attention and lower propaganda effects.

As we see, the two factions in Syria wage an information war in cyberspace. There are many organizational similarities, but the SEA is currently the stronger party. They enjoy a higher level of coordination and resources, and are able to complete a higher number of attacks both domestically and internationally. The opposition in cyberspace suffers many of the same shortcomings of the real world. Currently, the anti-regime hackers are loosing the Syrian cyber conflict. We will now move to descriptive analysis of the trends in the attacks during the course of the conflict, divided into three sub-chapter based on the findings of the case study.

Trends in Syrian cyber attacks 2011-2014

The following section will explain the main trends in the Syrian cyber attacks. This is divided into three sub-groups based on type of attack. It will also outline some main events, and discuss to what level an increase in sophistication has occurred since 2011.

As seen in the empirical record (see also the appendix), there are certain trends in the Syrian cyber attacks. We see that low sophistication attacks like DDoS, defacements and social media account hijacking is the most common courses of action for both factions. To date the SEA has a) hacked, disrupted, defaced and closed anti-regime websites both in Syria and abroad; b) spammed anti-regime social media with pro-regime statements; c) launched propaganda campaigns under Facebook aliases; and d) uploaded videos to YouTube to discredit the opposition (Khamis, Gold, and Vaughn 2014, 425). The anti-regime faction of the conflict also use YouTube, but not as part of a hacking strategy. Their actions tend to focus on government affiliates and supporters, and are mostly consisting of defacement, DDoS and data dumps. Additionally, the type of targets and attackers differ between the groups but include foreign governments, other hacktivists, or global news outlets. However, all the victims have in common that they are perceived as allies of the opposing party. The target selection is therefore based on perceptions, not facts. The data collected demonstrates that SEA has a much longer record of attacks than the opposition. This is probably due to two factors: a) the anti-regime group is less effective as they operate with a fractioned structure and fewer resources, and b) the attacks completed by the anti-regime are less likely to gain attention in international media as they mostly attack the regime, though some supporters have experienced DDoS and account hijacking. Consequently the attacks are mostly reported in Arabic, and are less likely to be part of the empirical record of this thesis due to the factors discussed in the methodological chapter. The international profile is also probably off less importance to the anti-regime faction as they already hold the support of the international community, whereas the SEA states that they desire to counter the current international coverage of the Syrian conflict.

Khamis, Gold and Vaughn (2014, 420) find a distinction between the regime's more traditional top-down approach to propaganda, which is balanced out by the cyber activities of its supportive non-state actors, and the bottom-up approach utilized by the opposition. It is therefore a central point that the pro-regime strategy enjoys the strongpoints of each

approach. The SEA contribution allows the broader approach founded in social media and disinformation campaigns. However, the leniency and possibly support of the regime allows for organizational strength and necessary resources. This case study also identifies two trends in the pro-regime narrative: a) the regime as the defender against imperial forces (exemplified by figure 3 and 5); or b) the regime as the strong, caring and brave father of all Syrians (exemplified by figure 4).

Figure 3: The leaders. From SEA twitter account 19.02.13

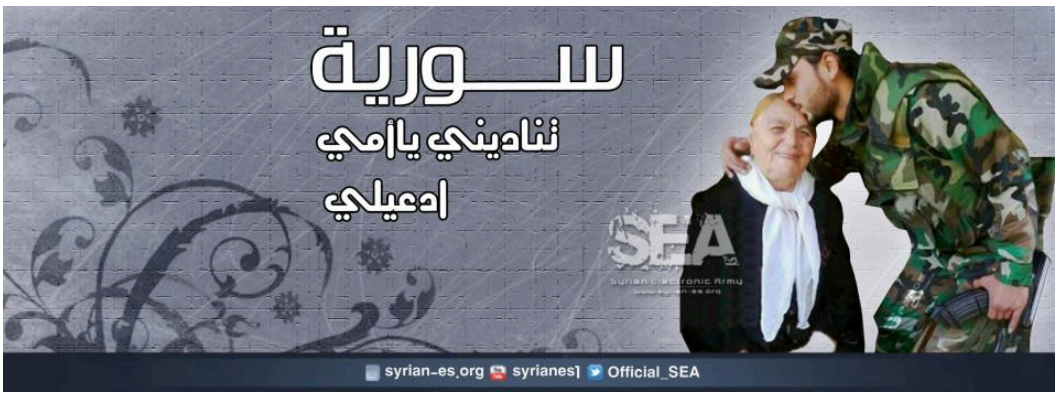

Figure 4: "Call on me Syria, my dear mother!" Picture from SEA website (http://www.sea.sy/images_gallery/en).

Figure 5: Syria vs. the rest. From SEA twitter account 29.08.2013 (https://twitter.com/Official_SEA16/media)

However, it has not been able to demonstrate an equally clear narrative in the opposition's operations due to the lack of empirical data. It appears at best more diversified, but a common message is that the regime is abusive, illegitimate and weakened. Both online and offline media is used to promote the narratives in the Syrian conflict, both depending on stories of torture, abuse and criminal activity (Khamis, Gold, and Vaughn 2014, 426). Both attempt to build perceptions of "martyrs", "criminals against the people", "victorious supporters". Assad additionally employ perceptions of historical injustices by claiming that the opposition is supported and financed by Western states and Israel, and maintain the argumentation of territorial integrity (Khamis, Gold, and Vaughn 2014, 429). Both sides use cyberspace to sell one's narrative, recruit new members and maintain existing support (Khamis, Gold, and Vaughn 2014, 431). This corresponds with the presented theory.

The empirical record and primary data collection show clear trends in type of cyber attacks, and significant difference between the two fractions. As presented in figure 3 and 4, the SEA has a more diverse and holistic strategy with distinct attacks in all three categories. The primary data concerning the anti-regime opposition however demonstrate a focus in the second category "data dumps, DDoS and defacements". As figure 9 demonstrates later, the opposition especially utilizes data dumps. This may indicate a defensive strategy rather then SEA's offensive. However, it may also indicate that the opposition focus on revealing human rights abuses and violence at the hands of the regime, thus attempting to subvert legitimacy as ruler. If the second interpretation is true, then SEA's work must be focused on hindering the spread of subversive information. Most likely, the strategies are a combination of the two. As further discussed bellow, the relative power is quite asymmetrical which probably leaves

the opposition to focus its resources on the potentially most beneficial course of action. SEA's resources and organization allows an offensive campaign to hinder diffusion of the subversive message.

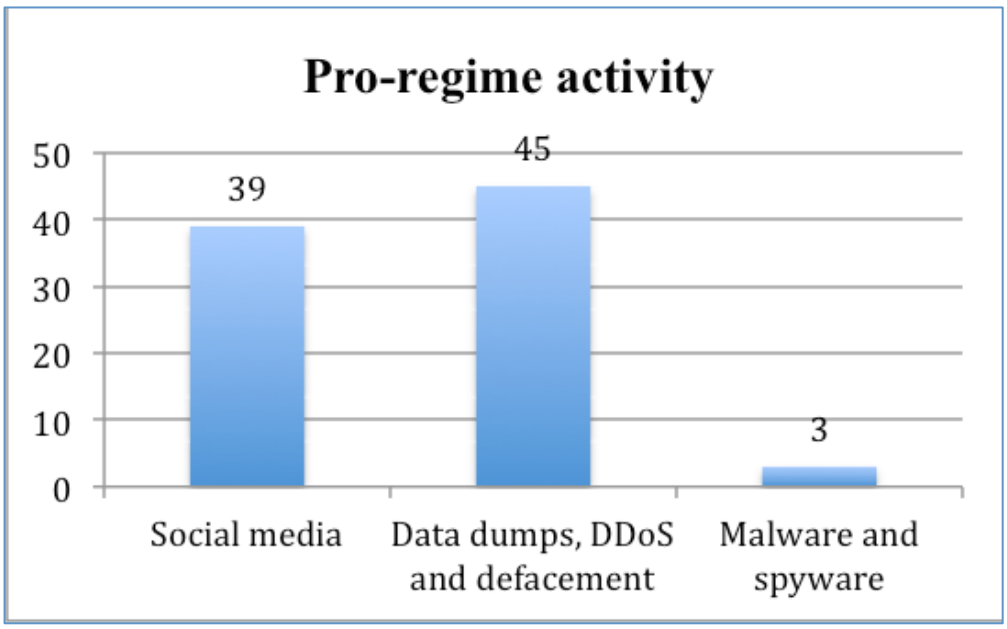

Figure 6: Pro-regime attacks in primary data by category

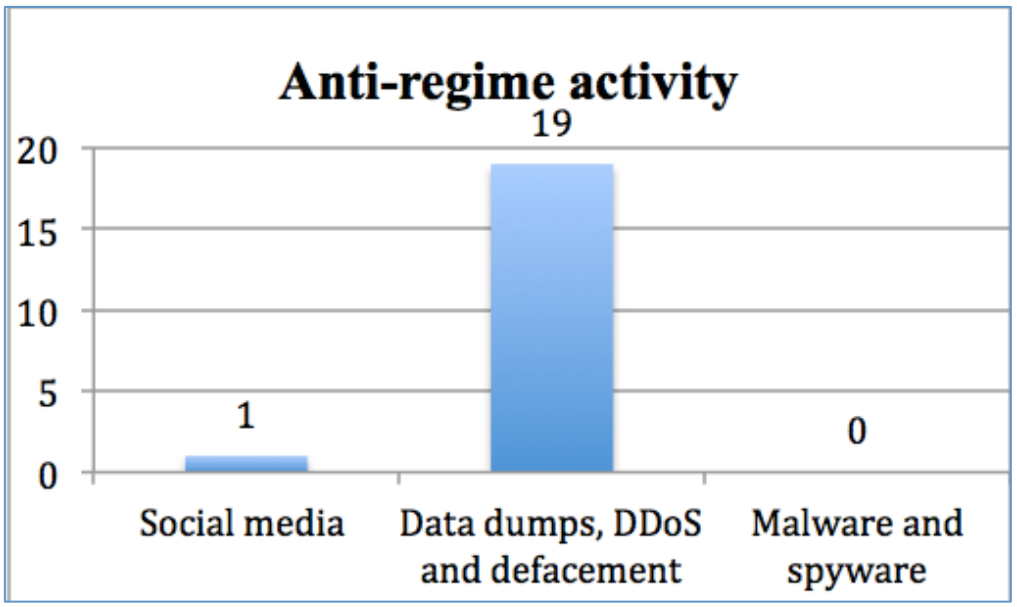

Figure 7: Anti-regime activity in primary data by category

It is also clear from the primary data and the studies referenced that the hacker communities Telecomix and Anonymous represent the greatest embarrassment to the regime, similarly to how SEA dominates the pro-regime fraction. This may to some extent damage legitimacy of as the Assad regime strongly push a narrative of the rebellion as foreign enemies of the Syrian state with imperialistic motivations. Though clearly not imperial forces, the international hacking communities dominance may create a perception of a weak and foreign-controlled opposition. However, this may also be of some advantage as it gives a perception of global support to the rebels. The alliance's consequences for the narrative and soft power are therefore unknown at the present time.

The case study will now take a closer look at the primary data and outline what type of action is undertaken. There are three sub-sections following the categorization of figure 6 and 7.

Social media

The empirical record in the primary data shows that social media infiltration is one of SEA's main courses of action. The opposition, however, seems to have focused their low sophistication attacks on website defacements and leaking information[84]. Consequently this section will focus on the work of the SEA. We see that especially Twitter accounts and Facebook profiles are vulnerable to account hijacking, but blogs and YouTube[85] also fall victim to attacks. Social media can be manipulated using specific software that is easily accessible, and this type of attack is therefore classified as of low sophistication.

In the beginning, in June 2011, SEA started a campaign to compromise and infiltrate opposition Facebook pages. They replaced anti-regime logos with SEA posts and pictures, claiming "bragging rights" for the intrusion. The number of fans of pages drops significantly after such infiltrations though the original title and structure remained (Noman 2011a). There are even accusations of individuals tortured until they disclose passwords for social media and emails (see also Baiazy 2012, 20), indicating the importance of this medium in the conflict. Intrusion of social media profiles has remained a key tactics in the conflict as the

[84] This corresponds with the track records of Anonymous in other cyber operations. Past operations tend to focus on Social Engineering (where individuals are psychologically manipulated to give access to systems or reveal log-in credentials), defacements, DDoS, or SQL injections and data-dumps (of private documents, emails etc.).

[85] It is true that the Syrian conflict has been called the "YouTube Revolution" and that this medium plays a key role, but it's importance stems from the number of videos posted and not their alteration and manipulation. Therefore this is not within the scope of this thesis, as it does not constitute as hacks.

SEA seeks to control the information available. While the websites suffer unauthorized alterations of content, the Facebook pages experience repetitive comments on multiple posts during a limited time to spread a specific message and dominate any dialogue occurring in the social media forum. The European Parliament, the European Union, the White House, the U.S. Department of State, U.S. President Barack Obama, French President Nicolas Sarkozy, Oprah Winfrey, Human Rights Watch, the al-Jazeera TV channel, al-Arabia TV channel, and religious scholar Sheikh Yusuf Al Qaradawi have since then all experienced these types of attacks by SEA. Additionally the SEA has hacked several major news and human rights organizations like BBC, CBS, AP, Reuters, Human Rights Watch; either leaving a signature logo or posting messages disguised as authentic news. The most dramatic event occurred on April 23rd 2013 when a fake AP twitter post read "Breaking: Two explosions in the White House and Barack Obama is injured". The Dow Jones fell immediately by 150 points and $136 billion was lost in market equity (National Post Wire Services 2013; Stalinsky and Sosnow 2013). However, when White House officials refuted this message, the stock market quickly recovered.

These attacks tend to correspond with the targets public statements against the Assad regime, and thus functions as punishment. One example is the correlation between Obama's public statements and SEA attacks on western media. CEO of Recorded Future[86] states to Mashable that it resembles

> Actions rebels sometimes take during wartime, such as using a radio station to stop presidents from talking. However, in this case, the radio station is the New York Times (Franceschi-Bicchierai 2013).

The following chart illustrates the correlation between Obama's public statements and cyber attacks by the SEA, leading Recorded Future to characterize the relationship as "propaganda warfare" (Franceschi-Bicchierai 2013).

[86] Recorded Future is a private company, which seeks to organize open source information for analysis. It focuses on cyber security, corporate security, and competitive intelligence. It is located in Arlington, Cambridge and Gothenburg. For more information, visit https://www.recordedfuture.com/about/.

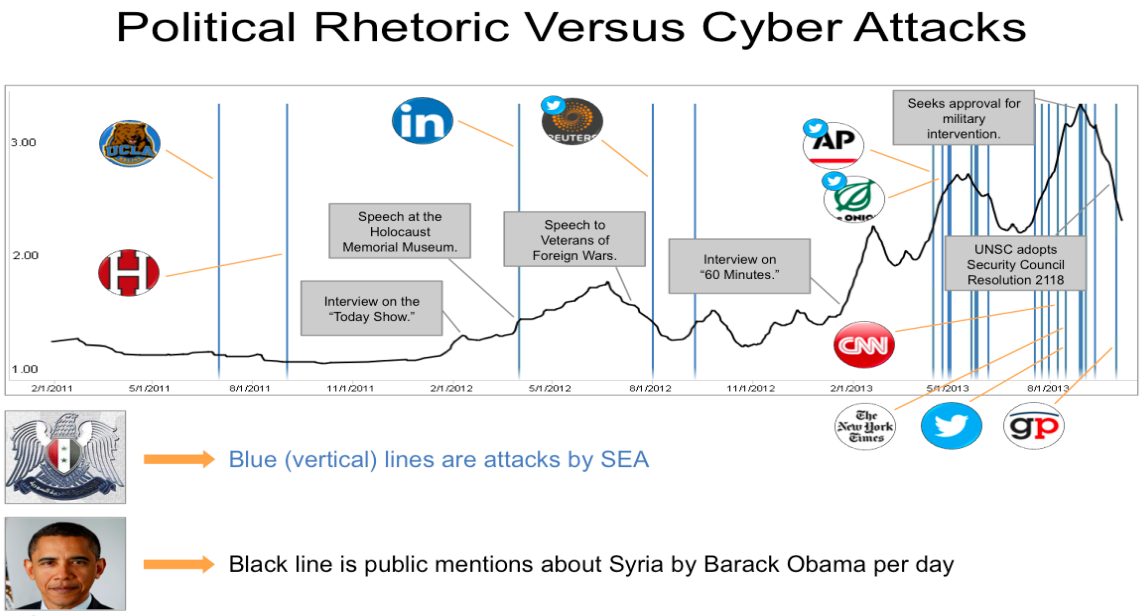

Figure 8: Political rhetoric vs. cyber attacks 2011-2013 (Recorded Future, republished in Franceschi-Bicchierai 2013).

Both pro- and anti-regime groups reportedly use mediums like Twitter to flood the conflict narrative with supportive statements, but as discussed SEA additionally hijack others' accounts. It is set up automatically by using so-called "spambots"; where computers automatically send out multiple posts a minute to drown out any unfavorable opinions (York 2011). The Twitter and Facebook pages are attacked for a number of reasons according to the group; for example to influence US public opinion, influence the level and perspective of media coverage, or in protest against supposed support of the revolution (Noman 2011b). SEA hackers have infiltrated social media accounts on multiple occasions to spread pro-Assad propaganda disguised as legitimate news. These types of operations usually target particular hash tags or social groups, and are a part of a manipulated narrative strategy to inflate the number of perceived supporters. Secondly, SEA's YouTube channel and Facebook page is used to create excitement around accomplished hacks and perceived victories. SEA also uses social media websites to recruit sympathizers that speak different languages (Noman 2011a). As we see from the empirical data, it may also be a way to override public warnings of circulating malware in online forums. The networks of automated "spambots" thus design a favorable environment where events are presented from only one perspective, creating the illusion of legitimacy. This is consequently a potentially effective propaganda tactic. To illustrate: 64 bots manage to post about 4 million pro-regime posts on Twitter over the course of four months (SECDEV Foundation 2012). They reduce the necessary resources

and coordination to secure the same level of exposure using humans, and create an impression of a strong support base and legitimacy.

There is no indication of fundamental changes in how this medium is used over the course of the conflict. Account hijacking is quite simple, and is usually facilitated through simple phishing schemes, demands few resources, and can result in massive attention and agenda setting. It is therefore likely that this medium will be used in the same manner in the future. However, one key development must be mentioned. There are some indications that account hijacking and social media are used to spread spyware and malware tailored for the opposition. Using fake or hijacked accounts, the SEA is accused of enticing anti-regime individuals to click on links or open attachments, which in the end gives SEA administrator rights for the targeted computer. Additionally they are accused of using "spambots" to drown warnings of spyware and malware circulating in social media. However, as social media is used as a delivery system, the implications of these attacks are discussed below in the section relating to malware and spyware. Some reports also claim that information obtained in these manners are used together with torture to secure regime agents access to social networking sites (Salhani 2013, 2). The stolen log-in credentials are used to spread propaganda, instill fear and destabilize communication-networks and gather information. Paralyzing information diffusion and destroy communication channels might then limit the movement's online scope and reach.

DDoS, defacements of websites and data dump

The first chapter of the thesis demonstrated that there are many ways to attack in cyberspace. However, the empirical record reflects that some dominate, which is most likely due to their low requirements to skills and organization, especially as automated malware is developed and spread through the Internet. This case study indicates that data dumps, DDoS and defacement are key tactics in the strategies of both pro-regime and anti-regime hackers, which corresponds with the technological situation in Syria. It is simple and does not require a high level of skills or sophistication. Additionally, more competent hackers publish "recipes" on how to complete DDoS and defacements online, thus guiding novices in how to complete such attacks.

As described in the first chapter, DDoS operates under the logic of a "flood". By spamming a server, it hopes to overflow the capacity and by consequence shut it down. It exists several types of software[87] that facilitates operations, and they are easily accessible online. Lastly, DDoS is also almost untraceable due to the use of VPNs[88], botnets[89] and proxy servers[90]. But the consequences are limited as the DDoS' are usually only effective for a short period. It is also relatively easy to prevent, mostly through filters that respond to sudden surges in activity (Sauter 2013, 17–19). However, successfully attacking popular websites it may create attention, which may be the goal of the perpetrator(s). We see in the Figure 9 and 10 that this method is common, but do not dominate the chosen action by either faction. This is probably as it more complicated to claim "bragging right". Defacement and data dumps however allow the groups to present proof of longer duration and create an electronic graffiti, which may be more in sync with the propaganda purpose of their actions.

It is somewhat ironic that the lack of resources has forced the opposition to turn the regime-developed DDoS software against the creators (Noman 2011a). From 2011 the anti-regime version was used to target sites such as the website of government General Organization of Radio and TV (rtv.gov.sy), Addounia TV station (addounia.tv), and Syrian news websites syriarose.com and syria-news.com (Noman 2011a). The original software was easy to use and only required some minor code alterations to be used by the opposition[91]. One such example is the "Syrian Gov Pigs (PIMPED BY XACKER)" version of the tool, where targeted websites easily could be overpowered for a limited time (Noman 2011a). This case study therefore argues, along with Sauter (2013, 40, 52), that like guerrilla attacks DDoS is most effective when complementary to a larger campaign. Especially the SEA has been rather successful in this respect, especially after they started to target international news

[87] With varying levels of sophistication, and both for purchase and free.
[88] A virtual private Network (VPN) increases the reach of a private network by connecting it through public networks like the Internet. By creating a "tunnel" it enables computers to exchange data as if they were located within the same closed network.
[89] A botnet (= "net of robots") is a collection of network (internet)-linked program that communicate with other programs to together solve a task. It is often done by robots, and facilitates large-scale spamming of commercials or to facilitate DDoS. Certain software can link multiple computers together and thus strengthen the capacity of an attack; this is done by so-called "zombie computers".
[90] A proxy server is when one machine operates as the intermediary between two others. By using this, the location and identity of the user can be hidden. It may also be a way of bypassing firewalls or access restrictions.
[91] Interestingly, in Syria the opposition has also made certain creative strategy choices. For example have they used the Google Crowd Sourcing program "Map Maker" to rename streets, bridges and other key places after their heroes. Lynch (2012) report that the activists do so to undermine the perceived reach and power of the regime, expunge the symbols of the Assad dynasty, and commemorate their fallen comrades (Khamis, Gold, and Vaughn 2012, 12). Though of little consequence, and easily retrieved, the symbolic effect is interesting.

media organizations. DDoS is also thus a useful tool for extortion, harassment and censorship (Sauter 2013, 10), as it blocks the information flow and can be a short-term nuisance. This control probably partly explains why the groups implement the tactic.

It is hard to identify a clear strategy in the anti-regime attacks, but it is clear from the case study that data dumps and website defacements are the most common types of attack.

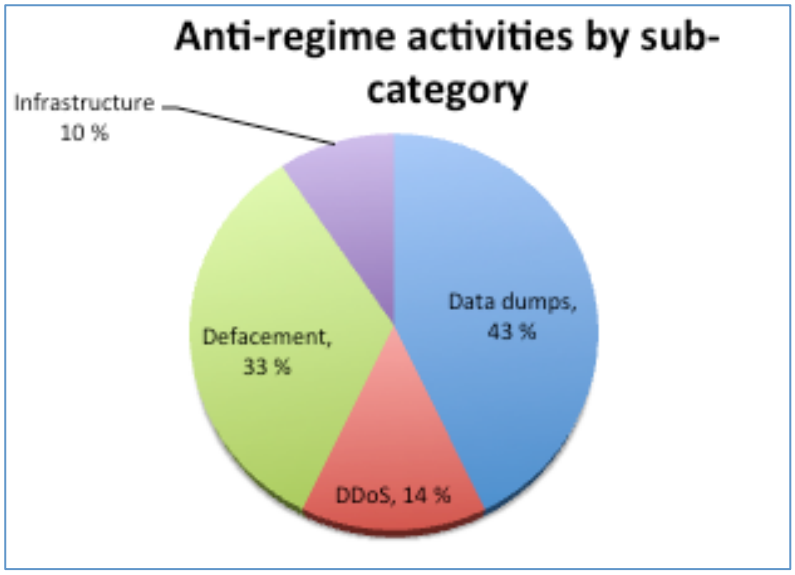

Figure 9: Anti-regime activity in primary data by sub-category

As seen, the anti-regime attacks are dominated by an informational component. One of the more active groups of late, Syrian Revolution Electronic Suite (SRES), has successfully attacked foreign governments that support the Assad regime. Both Kremlin's envoy to the Far East (www.dfo.gov.ru) and the Lebanese government have experienced attacks, where the hackers claim to punish these governments for selling weapons to the Syrian military or allowing Hezbollah to support the regime. Anonymous' first major attack in Syria was in August 2011, when members successfully defaced the Syrian Ministry of Defense's website (Salhani 2013, 3). Though of little consequence, it was an international embarrassment to the regime. Together with Anonymous and Telecomix, #OpSyria was launched as a global, anti-Assad effort in cyberspace August/ September 2013[92]. This became an international hacker

[92] Additionally Anonghost Team, an international hacker group, vandalized the website of the Syrian Ministry of Health (Hackers News Bulletin 2013), and an unknown group defaced the website of the Syrian State Media SANA.

campaign to signal support to the Syrian rebels, which also focused DDoS and defacements as weapons against the regime. Interestingly this campaign was launched after Assad threatened to shut Internet service in the country[93], bringing together individuals from around the world under the parole of Internet freedom.

In 2011 SEA organized a four day countdown before they defaced up to 130 websites (Noman 2011a). This led to massive international attention, and made defacement a tactic of choice also at later stages in the conflict. This research also finds that numerous attacks have targeted the websites of global news outlets like Al Jazeera, BBC, AP, Al-Arabya, usually simultaneously as phishing campaigns target social media accounts. A second campaign was launched in 2013 when SEA attacked several global news agencies (see also Chalabi 2014 or appendix for further details), claiming "media is going down" due to biased media coverage of the Syrian conflict. This type of attack is simple and easily executed but relatively effective. False stories and statements are posted as a means to disinformation campaigns, as well as creating attention for the group. According to the SEA, it does not seek to destroy websites permanently, only "voice the truth" (Noman 2011b). Sharing many characteristics with vandalism and graffiti, defacement has little effect on a conflict directly but may create attention and fame for the sender. The attacked western websites are not necessarily political, and reflect a strategy of opportunity similar to that of the anti-regime efforts. The SEA will favor the more prominent websites, but will attack whatever vulnerabilities they come across to get attention. This is a strategy that may be successful in creating the "fog of war", distrust and confusion, as defacement and alterations make it complicated to verify information and identify senders. Following NATO doctrine division between white, grey and black propaganda, defacement makes it harder for the recipient to distinguish between the genuine and truthful information and what is altered. If these consequences do not materialize, then the intrusion is at least a propaganda victory as it proves the opposing party's inability to secure and protect property.

[93] However, the Assad regime has closed Internet access on several occasions, but blames opposition sabotage or faulted infrastructure.

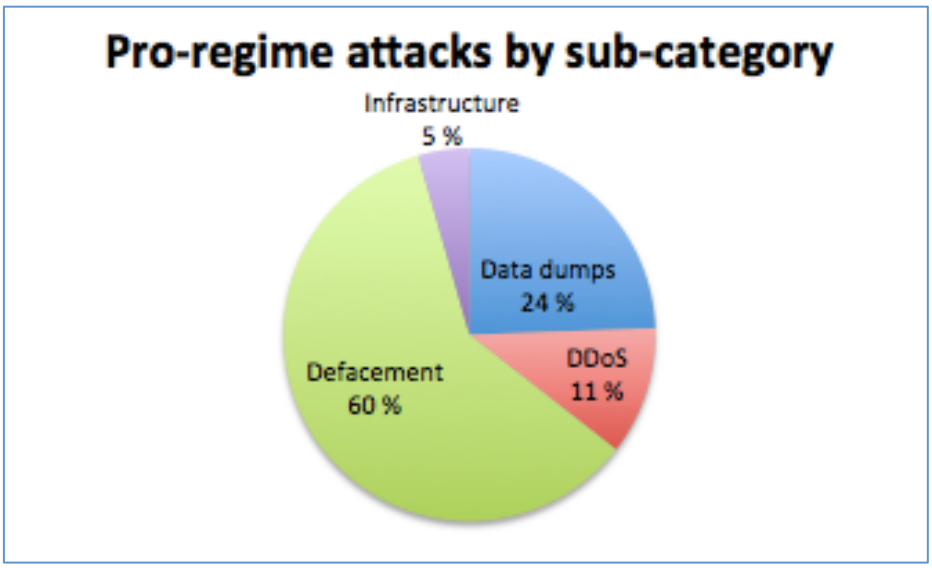

Figure 10: Pro-regime attacks in primary data by sub-category

In the beginning of 2013, it became clear that SEA had developed a new tactic to discredit the anti-regime movement. By publishing stolen documents from government servers in Turkey, Saudi Arabia and Qatar, the group hoped to provide evidence that the revolution was foreign backed and not "the people movement" the opposition claimed. The documents are of little security importance, but assist the SEA in building an image of transparency and legitimacy for the Assad regime (SECDEV Foundation 2013b, 1–2). Data dumps are also the most favored tactic by the anti-regime hackers (43% of registered attacks), who have embarrassed the regime on several occasions. The most noteworthy is the publication of President Assad's personal email on two occasions in 2012, and the publication of address details, phone number, more than 100 email addresses and encrypted passwords belonging to the Hayan Petroleum Company of Syria, and Anonymous' leak of SEA's servers.

Now moving beyond these low level attacks, we will see that a new trend in the Syrian cyber conflict. Espionage by software is becoming a more widespread, complementary tactic to the traditional online sabotage. Though not representing a new level of skills or sophistication, this is worrisome due to the potentially more serious, real world consequences for the individuals identified and targeted.

Malware and Spyware

The most serious form of cyber attacks seen in the Syrian conflict is by far spyware and malware. There are accusations that the software is used to identify and locate individuals, whom are later tortured or abused as "enemies of the regime" due to their support of the opposition[94]. Spyware and malware therefore resembles real world espionage at a higher level than the low sophistication vandalism of account hijacking, defacement and DDoS. The spyware also adds a second dimension to online sabotage, as it allows for a new level of impersonations. It is therefore likely that the growing use of spyware will lead to a growing self-censorship and distrust in Syrian cyberspace. While the two former types are aggravating and may serve a propaganda purpose, this third kind of behavior may impact individuals' lives and health directly.

Brumfield (2012) and Khamis, Gold and Vaughn (2012, 11) find that specific pro-regime cyber-campaigns are tailored to target the opposition's supporters, and that the information is returned to a server belonging to a state-owned telecommunication company located within Syria. The information obtained is then used for online impersonations, which allows for further spread of spy-Trojans into the communication network. According to the CNN,

> Supporters of dictator Bashar al-Assad first steal the identities of opposition activists, then impersonate them in online chats. They gain the trust of other users, pass out Trojan horse viruses and encourage people to open them. Once on the victim's computer, the malware sends information out to third parties (Brumfield 2012).

This case study, the Electronic Frontier Foundation (EEF) and Salhani (2013, 2) find that the pro-regime social engineering campaign is ongoing from March 2012. A coordinated campaign using software was also recorded by EEF in June 2013, but is believed to have started about six months earlier (Scott-Railton and Marquis-Boire 2013, 6). Online impersonations and electronic surveillance has therefore been incorporated as part of the counterinsurgency strategy for about two years. Cloned YouTube pages, interference on Facebook, and Skype and Adobe Flash Player malware are examples of the operations undertaken. The Information Warfare Monitor additionally reports that false URLs and log-in pages for social media networks are established to coax credentials and distribute hidden malware (Fisher and Keller 2011). It then spreads the malware to members of the network

[94] There are also accusations that online oppinions and private corrospondance are used as "proof" of anti-establishment behavior.

hidden in fake anti-Assad videos or documents. Opening these will install the malware, potentially give control of webcams and microphones (Siegel and Marquis-Boire 2013). The malware usually also take over control of the infected computer and gives access to files, online communication, emails, Skype conversations and Facebook chats. The campaigns appear coordinated as multiple attacks use the same RAT, named DarkComet, and the software report to the same Syrian IP address. The campaign also advanced by using another RAT, Blackshades Remote Controller, which allows registration of keystrokes and remote screenshots. There are also indications that the culpable is the same groups that stole social media log-in credentials in March 2012 by malware hidden in a fake Adobe Flash Player update (Galperin and Marquis-Boire 2012). A third RAT, ShadowTech, is also widely used (Scott-Railton and Marquis-Boire 2013, 6), which can be downloaded from both English and Arabic sites with instruction videos found on YouTube. The use of software must however not be interpreted as a higher technical expertise, and that we are moving towards the "cyber wars" discussed at the beginning of this thesis. The software is easily obtainable online as it is developed by a few skilled individuals and distributed to a greater network. Consequently one does not need a high technical competence to use such tools.

As described, Botnets allow for overload of networking profiles, flooding profiles with spam until they crash. It has been described as the most holistic response to online campaigns in the Arab Spring (Fisher and Keller 2011), forcing spread of pro-Assad narrative both domestically and internationally. Using automated "Zombie" Facebook and Twitter accounts, the spread of such malware may impact entire communication communities. As an illustration, anti-regime activists were targeted by a cloned YouTube website[95] that distributed malware, which both stole log-in credentials and left the attacker in command of the infected computer in 2012 (EFF 2012, in Salhani 2013). SEA is also accused of developing malware that targeted the Facebook interface and ultimately gave the developer control of profiles. This malware was spread by posting fake pro-revolutionary links, prompting "likes" and "shares". By visiting URL links, malware infected the profile, which then are used to spread pro-regime information under a false persona (Shehabat 2012). Lastly Skype has been the target of the mentioned Trojan "DarkComet (RAT)", which enables control of webcam, disables certain antivirus programs, record keystrokes, steals passwords

[95] The fake YouTube page looked similar to the real site, but prompted visitors to update their Flash update. When doing so, a hidden code trojaned a spyware into the victimized computer and gave full administrative control. According to the Electronic Frontier Foundation, the malware was most common in videos likely to be visited by anti-regime sympathizers.

and sends the information back to the attacker (Galbren et.al, 2012, referred in Shehabat 2012). This type of campaign, if lead by the SEA, is disturbing and indicates some development as the malware disrupts perceived secured connections and facilitate extensive surveillance. Thus tools the opposition uses to circumvent regime control is turned against them, adding yet another source of "the Fog of War". By attacking the communal trust, the center of gravity may also be damaged.

The case study shows that the anti-regime faction of the conflict is at a lower level of impact and sophistication due to lacking organization and resources. Some countermeasures have been implemented with international assistance, but these are limited to protective measures. Sites that explain in Arabic how to protect anonymity, secure online communication, and remove potentially dangerous online information have been developed, but this is more of a defensive measure while the SEA is clearly offensive. Telecomix further assists in moving pictures and videos out of Syria, and established a video portal for the spread of news (Khamis, Gold, and Vaughn 2012, 14). The European Cyber Army also claims to have caused a near nationwide internet outage in March 2014, though the regime blame a faulted optic cable (Peterson 2014). This study finds no record of spyware or malware by the anti-regime groups. It demonstrates the trends already discussed, with the SEA as the most active and offensive party to the Syrian cyber conflict. There are, as illustrated, many similarities between the anti-regime groups situation in cyberspace and the real world.

The Syrian cyber battle of narratives

The following section of this thesis will evaluate the state of the Syrian cyber battle. It will bring together the empirical record and evaluate the greater meaning behind the attacks reported. First it will look at the state of the current cyber battle of narratives. The second sub-section tests the assumptions of the thesis, and the third attempts to answer if the Syrian events qualify as a soft war in cyberspace.

The Syrian regime has clearly studied the course of events in Egypt and Tunisia. Having more time to prepare, Assad's followers reflect a clear narrative strategy where blocking information flow is key. However, they cunningly focused their efforts on certain times and locations to limit potential backlash and not to enrage the Syrian population. For example, Khamis, Gold and Vaugn (2012, 12) finds that Internet connectivity was initially shut down on Fridays, weekends and holidays in troublesome areas to prevent mass protests while limiting the potential economic losses experienced by the Egyptian government. After some time the Syrian regime also restored Internet connectivity (Shehabat 2012), but sophisticated filtering and censoring technology are used extensively. Despite the low penetration rate, Internet activity is closely monitored by the regime's surveillance system and the Syrian regime has a history of detaining citizens that express opinions or spread information online (Shehabat 2012). Instead of the neutral domain for information sharing and recruitment, cyberspace may become a honeypot to trap and infiltrate the opposition.

The SEA is spearheading the most visible cyber operations in the Arab Spring and provides an alternative to the Egyptian and Libyan regimes' response to rebels organizing online. These regimes closed Internet access, but failed as the opposition adapted and used proxies and dial-ups to circumvent regime-control (Fisher and Keller 2011). The Syrian conflict however is now as present in cyberspace as the physical world, and it may be the first regime in the region to target the potent effects of organizing counter-revolutionaries in this domain. Like this case study, a report by Citizenlab (Al Jazeera, The Stream Team 2013) also finds that the pro-regime hackers use a formula consisting of social media manipulation, malware, and remote-access devices. The regime supporters are thus able to halter operations by the opposition by manipulating many of the same online tools as the "people online-movements" use. Interestingly, they also target software formerly used by revolutionaries to circumvent

regime control. Consequently they turn the cyber weapons of the Arab Spring against the revolutionaries in Syria. They utilize global software as YouTube, Dropbox, email and Facebook to spread malware, operating outside of territorial borders and choosing victims based on ideological or political sympathies. The SEA is also interesting, as it does not appear to distinguish between international and domestic adversaries. Any organization or individual that appears anti-Assad is considered an adversary and eligible for misdirection, espionage, or sabotage.

This case study shows that the pro-regime fraction of the conflict, exemplified by SEA, has recorded over 80 attacks that have been reported in foreign media. Several additional attacks are also recorded in the secondary data. It is likely that the real number is much greater, but that these have not gained the desired attention in international media and the research community. Analysis Intelligence also records a tenfold number of references to SEA compared to any other actor in 2013 (Holden 2013), much due to its massive campaigns targeting international highly profiles in the first six months of the year. This is an impressive number of successful attacks at the hands of a minor group consisting of only a few members[96]. By targeting people like President Obama and global news media, the SEA secured high coverage and continued reporting on its activity. As the case study has shown the main type of victims is news media, attacked due to their portrayal of the Assad regime.

The most sophisticated attacks to date are the hacks of US military. While the first was only a defacement of the US Marines website (in September 2013), the second was illegal access to the military knowledge base CENTCOM[97] (in March 2014). This attack is at the time of writing yet to be confirmed by the military, but analysts agree that the pictures published indicate that the SEA penetrated the web portal. It is unlikely that the documents accessed were of great national security importance, but the propaganda effects were considerable. This research also indicates that this was SEA's goal when targeting CENTCOM, as they were aware of the massive attention such a breach would conjure. SEA's many attacks have also placed the group on the FBI's terrorist lists (Neal 2013), giving the group even more

[96] According to their new website (04.04.14) the key members are "The Soul", "Vict0r", "The Shadow", "TH3PR0", "Syrian Eagle", "TH3MUS3", and three additional unnamed individuals (SEA 2014).
[97] U.S. Central Command (CENTCOM) is one of nine unified commands in the United States military. Six of these commands, including CENTCOM, have an area of responsibility (AOR), which is a specific geographic region of the world where the combatant commanders may plan and conduct operations (CENTCOM n.d.)

fame. Lacking sophisticated technical capability, Holden (2013) categorizes their work as "a guerrilla public relations campaign to put pro-Assad propaganda in front of western readers".

The case study indicate SEA's hacking strategy in the beginning was divided into three focus areas: a) defacement attacks against Syrian opposition's websites; b) defacement attacks against western websites; and c) spamming popular Facebook pages with pro-regime comments (see also Fisher and Keller 2011; or Noman 2011b). The current SEA website, launched in the spring of 2014, divides the strategy to three somewhat similar axes: a) Twitter propaganda, b) Facebook propaganda, and c) hacks of any Assad enemy. Though the past low sophistication attack strategy has continued, SEA's change in organizational structure from late 2011 has also led to a greater focus on international victims. Over time they have also broadened their scope, now claiming that any information that reflects negatively on the Assad regime is considered "hostile" and a fabrication of facts (SEA 2014; SECDEV Foundation 2013a, 3). Secondly, defacement is replaced with propaganda as the most important purpose. This may indicate that the role of the narrative has gained importance at the cost of simply controlling the flow of information. The changes in organizational structure may also have lead to new expertise and human capital, thus allowing more proficient hacking than simply attacking through spearfishing. Now the group is for example able to exploit vulnerabilities in WordPress software. They also have gained access to surveillance spyware like "Dark Comet" and "BlackShades" (Perlroth 2013). Disguising an encryption service within Skype requires some sophistication, but this must not be interpreted that the group has abandoned its former low-sophistication tactics. These still forms the majority of SEA attacks today[98], and no attacks recorded in this case study can be classified as high sophistication. However, the softer effects may still be real. Surveillance may seriously hamper the work of the opposition, and imposes a self-censorship as it is impossible to know how is watching. Potentially Big Brother may always see you, obviously

[98] The Syrian government however focuses their efforts on identifying and tracking opposition members, much helped by cyber tools. The Syrian government launched in 2011 a wide reaching software system targeting emails and Internet website traffic. The investment cost the regime more than $7.2 million and was sold by the Italian company Area SpA. It depends on the technology of Hewlett Packard and NetApp Inc. (both US based companies), Utimaco Safeware AG (Germany) and Qosmos SA (France)(Baiazy 2012, 20). The system includes capabilities for installing probes in mobile- and Internet providers, mapping of contacts, and hacking emails accounts (Baiazy 2012, 20). Iranian experts have also trained Syrian technicians in Internet surveillance, and these tasks are a potential "safe" way of completing the 18-month conscription duties (Baiazy 2012, 20). It is likely that the SEA is either involved or assisting in this surveillance campaign.

a terrifying prospect for any anti-regime establishment. As discussed, the links between SEA and the regime are unclear, but again we see that they mutually benefit from each other.

The case study shows that the anti-regime attacks are fewer and have less impact. This is because the Syrian society lacks the necessary civilian human capital to wage a cybered conflict between equal fronts. We have seen that Syria has a short technological history and a strong tradition for control and censorship online. The regime routinely block global sites and social media, controls the infrastructure, intimidates bloggers, and has a higher capacity in use of surveillance software. In sum this leads to a more asymmetrical online conflict in Syria than what was experienced in Egypt. From May to June 2011 the opposition could do little more than produce some videos (see also Khamis, Gold, and Vaughn 2014, 424), while the regime studied the Arab Spring revolts with care. Though the use of social media as a platform for information sharing was quickly adopted, the element of hacking was not included. However, after some time, the opposition increased its sophistication with help from the diaspora and international hacker communities (Khamis, Gold, and Vaughn 2014, 424). Today, though of small measures, the opposition has successfully hacked and published President Assad's personal emails, web defaced the Syrian Parliament website, completed DDoS attacks on TV stations like "Al Donya", and removed SEA's Facebook pages on several occasions in 2012 and 2013 (Shehabat 2012). In total, SEA has been forced to re-launch their Facebook page more than 239 times; mostly due to mass reported complaints on SEA violations of Facebook Terms of Use agreement. It is likely that the opposition targeted social media as their resources limited their options, and removal of the social media accounts allowed for disruption in the pro-regime information flow. However, this research also indicates is that the pro-regime groups responded by taking use of more sophisticated tactics like online sabotage and surveillance, thus crushing potential developments in the anti-regime opposition's level of sophistication. Though they still lack the necessary unity and skill, with the help of international hacker communities, they are more effective in launching campaigns that gain attention while hiding from the regime. Thus the opposition has, like the anti-regime groups in the real world, depended on aid from abroad.

This case study illustrate that, at the present time, the pro-regime non-state actors are winning the cyber battle. However the anti-regime activists also have a great presence in cyberspace, though more in social media and video sharing websites then hacktivist activities (Bogart

2013)[99]. New media is therefore used to promote the movement and discredit the regime, as the protesters have seen succeed in both Egypt and Tunisia (see also Rogan 2011, 483–499). The focus is thus to counter the regime's presentation of events and issues, and to influence international news agencies' reports of the Syrian conflict. This is also why the anti-regime attacks have focused on data dumps, hoping to provide proof of an unjust regime. However, the Syrian regime and its supporters have evolved and adopted cyberspace as a domain of narratives. The anti-regime groups have however not demonstrated sufficient innovation to counter the more prepared Syrian regime, compared to Egypt and Tunisia. They have thus not been able to define the form and field of battle, as found by Arreguin-Toft to be they key to success for the weakest party. Both the theoretical foundation and the case study has shown that a key element in any conflict is to shape the understanding of the war's causes, chronology and perceived winner. Attention can thus shape both policy and agenda in a hamlet, a country or the international community. Cyberspace provides a new medium in which the opposing parties attempt to shape perceptions and write how history is told. By forming the conflict narrative, the long-term political effects are therefore in theory infinite. However, as the effects are beyond the scope of this thesis and to complex to measure at the present time for the ongoing Syrian conflict, we must conclude that the international perception is possibly affected, not shaped, by the work of the SEA and the opposition groups. We will now move to the assumptions and to what extent they are supported by the case study.

[99] As social media presence is not the object of study in this thesis, such empirical record has not been included.

Testing the assumptions in Syria

The research question guiding this work is *"why and how do non-state actors use cyberspace in modern conflict"*. The following section of this thesis will evaluate to what extent the underpinning assumptions are proven true in the Syrian case. As we remember, they were summarized by five statements: (1) Non-state actors use cyberspace in conflicts; (2) Subversion is the ultimate goal of their actions in cyberspace; (3) This is done by spreading a strategic narrative and build soft power; (4) To reach their goal, they use guerrilla tactics; (5) The effectiveness is determined by level of organization and resources.

The case study clearly demonstrates that non-state actors use and manipulate cyberspace in the Syrian conflict. There are two structural reasons for this. Firstly, technological advances are fundamentally altering the mechanisms of asymmetrical conflicts (Wallace and Reeves 2013, 1). The covert warfare currently taking place in cyberspace thus resembles to some extent the covert operations of the Cold War (Kallberg and Thuraisingham 2013, 7). Attacks are undertaken by an unknown adversary, aimed at sabotage and espionage as part of a greater strategy. Secondly and the most relevant for the first assumption is the fact that, in cyberspace, individual actors and loosely connected groups have advantages if holding limited goals of strategy[100](Nye 2010, 13). As attribution is complicated and the environment of cyberspace resembles a maze, the non-state actors are able to facilitate hit and run operations where they may gain attention and inflict damage with little fear of consequences. For the same reasons it becomes an ideal environment for states to enlist the help of non-state actors or for non-state actors to coordinate political movements[101]. The non-state actors are therefore able to secure attention and have effect beyond what their relative position entails.

What the case study also has shown is that it is not the intention to undermine their opponent to the level of conquest. It is therefore not a domain of war, but one of conflict for the non-state actors. Remembering the cyberwar debate in the theoretical chapter, this thesis thus

[100] Attacks with great consequences (like Stuxnet) demand to many resources to be completed by these types of groups, sponsorship by greater organizations are therefore required. However the groups discussed in this thesis tend to limit themself to "cyber hooligan behavior" like defacement and DDoS, which are not that technically challenging. Additionally the loose confederation limits the risk of detainment.

[101] Though reality of lethal cyber war may be questioned, the effects are negative. For example are cyber espionage and sabotage becoming the most pressing threats in cyberspace today (Mulvenon and Rattray 2012a, xiv–xv; Rid 2013), costing both strategic edge and economic gains. As resources to an increasing extent are located in cyberspace, the denial of services (DDoS) is also becoming an integrated part of conflict as seen for example in Estonia 2007 (Mulvenon and Rattray 2012a, xv).

rejects the belief of cyberspace as a fruitless domain for war. This can only be true if measuring success as defeat in the real world due to actions in cyberspace. This case study however demonstrates that this measurement of success is faulted, as the non-state actors use cyberspace as a domain for distribution of narrative in conflicts. The real effects of non-state combat in cyberspace is thus not linked to "cyber Pearl Harbor" and other doomsday scenarios, but as a domain for the propaganda and subversion. However, the potential destabilizing effects are also limited and it is therefore unlikely that cyberspace will become an independent domain of conflict. A more likely scenario found in this case study is therefore that cyberspace provides a mouthpiece with little costs, risks and global reach. Publicity, image-building and propaganda distribution therefore becomes the measurement of success in cyberspace, working in tandem with the action on the ground.

The case study has clearly shown that the goal of non-state actors in cyberspace is attention and to gain legitimacy. Especially in the case of SEA, this strategy is clear. This is probably also why they focus their efforts on foreign actors, as this gains more international attention and force their agenda on the international audience. Also, the current anti-regime cyber forces do not present a genuine opponent as the SEA currently dominates the Syrian cyber conflict. This case study indicates a compromise as the domain provides fewer risks than engaging in real world combat, but simultaneously the power of agenda setting is questionable. Attention is their ultimate goal, but they can only choose to attack victims that create attention (international media) but have little control over what level and type of attention their actions result in.

SEA, as the most likely case, it should be clear that non-state actors use cyberspace as a domain for conflict. Regardless, even the most active and sophisticated group SEA, has a limited reach and the impact of their operations is questionable. Therefore it is a tentative conclusion that the SEA, and possibly similar groups, attacks what can be described as "low hanging fruit"; targets that are rather easy and hope that this will create the outcome they desire. To call them powerful however, will be wrong as they have little control or ability to shape others' behavior, perspective and responses. Their power is limited to an attempt to form a favorable environment to present their subversive argumentation. Thus we must conclude that it is at best a contributing factor. It can be understood as an "informational guerrilla movement" (Castells 1997, 79) or "social netwar" (Ronfeldt 1998, 1), where the actors utilize the traditional hit and run tactics and guerrilla strategy to play to their strengths

in an asymmetrical information war. As we saw at the beginning of this thesis, subversion refers to the (attempted) breakdown of social bonds where social rules and principles are altered. This is undertaken to undermine a system, a community or a group. This case study has shown that the non-state actors attack each other to damage the opposition's relative power and position. By undermining their role domestically and/or internationally, they hope to win the informational propaganda war undertaken in cyberspace. The case study thus indicates that non-state actors in cyberspace primarily try to impact on the softer side of warfare, meaning how it is perceived[102].

The case study also shows that the non-state actors do not require a high level of sophistication to gain attention. Independently the cyber attacks are an annoyance, but together they may create a subversive campaign and may contribute to undermining the standing of a regime or an opposition group. Especially in repressive regimes the cyber attacks of anti-regime groups can embarrass and undermine the ruling elite, possibly facilitating real world rebellions. Cyber operations of low sophistication can also help build an image on the international stage, possibly creating perceptions of relative strengths and legitimacy. At a lowest level, the attention and use of spambots may drown opposing opinions[103]. They seek to gain attention for their operations to project an image as undefeatable, and to frighten their opposition. The perceptions are therefore demonstrated as more important than the actual course of events. The case study has shown that especially the SEA is rather successful in gaining attention though, as previously discussed; they cannot be labeled as powerful as they cannot control the responses to their actions. They can however promote a favorable perception, where their narrative is seen as "the truth". As the country is in the middle of a civil war, confirming and refuting allegations is next to impossible. The truth is therefore less important than perceptions. However, as we have seen in the case study, regardless of domain, the effects are complicated to measure and uncertain for soft tactics like propaganda and narratives. Therefore the case study indicates that subversion is a goal, but its realization unknown.

> We can expect more from all directions. In war, the greatest casualty is the truth. Each side will try to manipulate information to make their own side look like it is gaining while the other is losing (Fitzpatrick 2012).

[102] Any violent effect of subversive operations in this domain is ultimately indirect and uncertain. In consequence, violence may be orchestrated through cyberspace but the effects are not guaranteed.
[103] However, as noted, such a campaign can be impeded by rather easy means such as surveillance software and contra-cyber attacks.

As we see in Syria, attacking media can be an effective way of securing greater attention than the groups standing is due. By using social media and manipulation of online communication channels, the groups are able to reach a greater audience. Also the accusations of impersonations and cooperation with the regime may prove sufficient in deterring supporters to join the cause, regardless of the truth to the relationship and extent of information sharing. Consequently the narrative of strong cyber "police" may instill fear, and their extensive media coverage confirms their presence and level of activity. So, regardless of the regime's relationship with the SEA, the mere rumor of its' existence may prove potent. This may also be a way to spread a message of fear similar to the "night letters" seen in Afghanistan. David Kilcullen calls this "armed propaganda", where brutal actions enforces the effects of communication strategies (Bøe-Hansen 2010, 36). The fear of retaliation can spread much further than to the actual recipient of the letter, thus increasing the effective use of resources and power projection.

The non-state actors focus their resources and efforts at the second level to build a different form of public discourse than what would happen without interference. Domestically both parties challenge the others' narrative and hinder diffusion either by blocking the necessary infrastructure or by embarrassing the other by publishing personal emails and pictures, circumventing their obstacles and promoting a subversive domestic discourse. Perceptions and the battle of hearts and minds is a clear variable in the Syrian conflict, a society with a fractioned population and an opposition lacking leadership. There is an ongoing battle of perception and narrative between the parties, both targeting the population and the international audience (Nissen 2013). The argumentation either builds on the legitimate right to uphold law and peace in the sovereign territory or, or the right to rebel against unjust leaders. The enemy is either described as foreign-backed criminals without respect for law and order, or as maniac regime run by corruption and oppression. Both use video and photos actively to present stories and evidence supporting their narrative. Common is also proof of inhumane behavior at the hand of the other (Nissen 2013, 77), thus legitimizing the struggle for survival of the sender. The Syrian cyber actors vary greatly in their success in gaining attention for their cause, with SEA currently winning. However their greatest success in the battle of the narrative is limiting the work of the opposition by damaging sabotage and espionage. The lack of major defections from the regime also indicate a continued support for the Assad government, and the volume of cyber attacks by the SEA may contribute to a "band-wagon" effect where the perceived support of the regime is high. This may in turn

encourage others to support the regime. Both sides of the conflict paint the other as brutal and dangerous, also possibly creating a sense of hopelessness for the unaligned individuals who in turn do not support either.

> History, as they say, is written by the winners. Information warfare, then, is effectively about good PR. But in a wartime environment, elements of kinetic conflict and information dissemination are inextricably linked. The battle is for control of the media, but in the early 21st Century, even that term is far more nebulous than before. The channels for disseminating information have exploded into social media, websites, VoIP communications and videoconferencing (Bradsbury 2013, 16).

By claiming that the opposition is supported and lead by foreign powers, the SEA seeks to undermine the revolution's legitimacy. The opposition on the other hand claims to be representatives of the people, and naturally SEA and the regime refutes this. Secondly, its' cyber operations builds a perception that the regime is still strong and should be feared. Thirdly, by spreading accusations of human rights violations at the hand of the opposition the regime is able to undermine the moral authority of protesters against a despotic regime. In total, these factors may contribute to regime recruitment or passivity in the citizenry but obviously the results are next to impossible to measure at the current time, and are therefore simply speculations.

The Syrian conflict is the most socially mediated conflict in history (Lynch, Freelon, and Aday 2014). Simultaneously as individuals believe that they receive unmediated information through these mediums, and the content of social media is re-reported in mainstream, traditional news. Together this makes the manipulation of social and online media valuable as a target. The massive attacks on social media platforms and news media indicate that the Syrian non-state actors actively use cyber attacks to shape perceptions and frame events. This is true for both sides of the conflict. Also the manipulation of stolen social media profiles by the SEA demonstrates the importance of such behavior. By using online impersonations they promote their narrative and exploit the credibility of whomever their stolen profile belong to. The fear of being ousted to the regime by liking and sharing videos distributed by false persona, may deter supportive individuals from contributing similarly to how we see criminals fear infiltration by law enforcement.

> Propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist (Jowett and O'Donnel 1999, 6) [104].

Telling the best story, thus presenting the most appealing narrative[105], is a key element to winning new wars (Leuprecht et al. 2010, 42). This must be tailored to a specific audience and follow the same structure as most fairytales: some are good, some are bad, grievances must be revenged and if following a certain recipe one will "live happily ever after" (Casebeer and Russel 2005, 1–5). Common tactical steps to build a narrative are presenting the targeted group with a terrifying threat, reports of attacks and abuse, a dehumanized the opposition, and framing support as the only viable position (Nissen 2013, 76). Narratives also utilize tactics like name-calling, in-group mentality, generalities, burial of opposing evidence, and calls for others to join the cause (Maliukevičius 2006, 139). Actors use this strategic narrative to justify claims and motivate action, assisted by culturally shared beliefs and understandings (Garrett 2006, 206).

We see clearly distinguishable narratives in the Syrian conflict, actively pushed in all forms of ICT. New technology has expanded and changed the role of communications, and the possible channels to spread a narrative. This makes media skills, persuasion and socialization fundamental in contemporary conflict (Castells 1997; Keck and Sikkink 1998, referred in Garrett 2006). The case study has also demonstrated that especially the SEA has insights into the opposition's emotional and societal preferences. They tailor their operations to wherever and whatever software that is likely to be used by the opposition, thus dominating the environment. By focusing their efforts in the domain favored by insurgents in Egypt and Tunisia, the power of this domain has been not been realized for the Syrian opposition groups. Sophisticated social engineering based in a deep understanding of the opposition's needs, interests and weaknesses (Scott-Railton and Marquis-Boire 2013) is therefore a common theme in the attacks of the SEA. They identify themselves as the "underdog" and the "righteous warriors" fighting the dangerous villains that are destabilizing their beloved Syria. They truly believe that they are "the last frontier" (Furlow and Goodall Jr. 2011, 218),

[104] It is further divided into white, gray and black propaganda depending on to what extent the sender of information is explicit.

[105] Narrative as used in this thesis signifies strategic narratives. This is understood as "a tool for political actors to change the discursive environment in which they operate, manage expectations, and extend their influence'; they are 'representations of a sequence of events and identities, a communicative tool through which political actors, usually elites, attempt to give determined meanings to past, present and future in order to achieve political objectives" (Miskimmon, O'Loughlin, and Roselle (2012, 3-4), quoted in O´Hagan 2013, 561).

chosen to fight as an answer to a higher calling. They manipulate emotional considerations and tailor their attacks to fit the ideology or curiosity of the targeted victim. Sharing videos or documents with titles like "Assad's Human Rights Abuses", the malware easily spread within groups that object to the current regime. As log-in credentials are stolen it is also difficult to trust any sender of information, and as a force multiplier malware is now hidden within software that is suppose to circumvent regime surveillance.

> The legal and technical restrictions, as well as the climate of fear are shaping the discourse online (Bogart 2013).

Narrative's argumentation often bases its arguments in past injustices and future horrors (Furlow and Goodall Jr. 2011, 219), dehumanizing the enemy. Assad has continuously accused the rebels of tearing the country apart, and presented his regime as the only solution and leadership possible (Shehadi 2013). In Syria's cyber conflict, the turbulent history of the country and its former victimization to imperial forces are manipulated to argue a narrative of Assad as the protector who secures the wellbeing of all Syrians. Also tapping into past grievances (Rogan 2011), this type of narrative has great resonance in the citizenry for both historical and cultural reasons (for a detailed overview of Syrian history, see Rogan 2011). The opposition is therefore branded as foreign backed troublemakers, only interested in enriching themselves. By using the hatred of Israel and the US, as seen in the Twitter pictures presented before (Figure 5,6 and 7), a conspiracy is narrated. This narrative justifies actions and certain behaviors, as it creates a perception of injustice and what Stout (2004, p. 1; in Furlow and Goodall Jr. 2011, 215) calls "self-righteous violence". The actors attempt to undermine the position of "the other" by character assassination and name calling, white and black presentations of moral issues, and self-proclaimed moral superiority (Wilcox, 2005; in Furlow and Goodall Jr. 2011, 217). The argumentation builds on the belief that the sender has the only solution to an essential problem, and the solution is based in an ideological belief that often justifies some use of violence "for the greater good".

> The Syrian opposition worked hard to craft a narrative for the international media of a peaceful, pro Western uprising, and the Syrian regime sought to portray their challengers as radical Islamists supported by nefarious outsiders (Lynch, Freelon, and Aday 2014, 8).

Throughout the revolution, the Assad regime has used its stronghold in the media to push a narrative of the revolution as a western conspiracy lead by USA and Israel (see also Khamis, Gold, and Vaughn 2012, 9–10). This narrative is further pushed by SEA in its online publications, as illustrated by the pictures presented before (Figure 3, 4 and 5). Lync et.al

(2014, 10) however finds that the same is true for all fighting groups in Syria. They develop tailored narratives appealing to their demographics. For example, a secular activist pushes a narrative of the opposition as a moderate force opposing human rights abuses to attract western support, whilst Islamist groups highlight the importance of Sala and Jihadist spirit to secure funding from Kuwait or Saudi Arabia. The narrative serves as inspiration, motivation, and provides a raison Raison d'être for fighters and supporters alike. In sum, it builds a bridge between "hearts and minds" and the physical world.

Large governments depend on large systems, political support and soft power. Non-state actors however are not limited by these constraints and may adapt "hit and run"-tactics as traditionally seen by guerrilla movements due to their flexibility (Nye 2010, 13). The consequences may be limited, but if the aim is disruption and attention then its realization may not be hard. The parties in this case study utilize hit and run tactics to build a subversive momentum against the stronger party. At the time of writing the stronger party, SEA, is the most successful but also this group uses guerrilla tactics. The anonymity, low costs of entry, and the asymmetry of vulnerability and power; all nurtures the position of Syrian non-state actors in cyberspace.

The case study demonstrates that the actors use the same guerrilla tactics as in real world conflicts, and follow Mao's recommendation of melting into the citizenry. Hit-and-run attacks, deception, sabotage and espionage are all used to push ones' agenda. Their attacks are minor and small-scale, characterized by opportunity. They also seem to favor civilian targets, as these are less protected, much as traditional guerrillas. Due to their relative weakness, they are not able to challenge the military command and control systems. This demands another level of expertise and sophistication than available, but by focusing on media and prominent individuals, they are able to obtain the desired attention with the means available. Remembering the understanding of guerrilla warfare described in the beginning of thesis, we see clear similarities between guerrilla warfare in the real and virtual world. Also remembering Arreguin-Toft's work, the weaker party may be successful is refusing to follow the rules of the relatively stronger party. However, the more resourceful party, SEA, is winning as the opposition is operating within a conflict parameter decided and controlled by SEA.

The actors themselves also show similarities with our traditional understanding of guerrillas.

They are characterized by loose organizations with some formal structure. However, the individuals are volunteers that decide themselves the level of commitment to the cause. They avoid direct confrontation with each other and the military establishment, except in the case where the SEA hacked the US military. However, the more sophisticated event is still limited, as they did not gain access to documents of national security and cannot be categorized as a military provocation.

> Cyberspace is unlike traditional warfare, but it shares some characteristics with the historical role of aerial bombardment, submarine warfare, special operations and assassins. Specifically, it can inflict painful, asymmetric damage on an adversary from a distance or by exploiting the element of surprise (Geers 2011, 12).

Both parties use the guerrilla tactics presented at the beginning of this thesis, but with different levels of success, much as seen in the real world. Also similar is the focus on attention instead of determining the outcome of the conflict, as illustrated by the anecdote of the fly exhausting the dog that was recited in the first chapter. We see that the actors use hit and run tactics, playing to the strengths of a flexible network organization, and immerse themselves into the civilian population and their domains by using social media and news sites. The target selection, appearing random and of opportunity, may be just that. But this is also an example of guerrilla tactics where the warriors attack whatever facility or site possible. Nevertheless the growth in SEA's sophistication may indicate a move towards an organization resembling the militias[106] or private vigilante committees of the real world. The anti-regime groups' lack of coordination, organization and resources make their strategy, or lack thereof, resembles "cyber hooligans" or "cyber vandals" that are less coordinated and operate at random. Lastly, the case study indicates that the various groups in the Syrian conflict enjoy and suffer much of the same realities as in the real world. The opposition suffers from internal disagreement and conflict, few resources and little human capital. In comparison the pro-regime faction appear stronger and has a strategic advantage despite its low level of sophistication. Though the effects of their campaigns are indefinite, it is clear that the SEA has a more holistic use of the guerrilla tactics discussed. The opposition appears less coordinated and dependent on foreign assistance, resembling groups not yet developed to the level of a cyber guerrilla.

[106] Militias refer to a military force that is raised from the civil population to supplement a regular army in an emergency. It is therefore not synonym with the current SEA, but the group may evolve into something resembling this definition in the future.

Until mid- 2013 the pro- and anti-regime groups pursued similar tactics of hacking each other and others. However, the case study shows that their targets have overall varied some. SEA and other pro-regime groups overall have focused on gaining attention by DDoS and defacement. The case study also demonstrates that the SEA evolved from late 2012 throughout 2013, and has refocused their attacks to a more international profile, developed a higher level of organization, and formulated a holistic strategy. The anti-regime groups have however focused their hacking activity at obtaining and releasing private and government documents violations (SECDEV Foundation 2013b, 2–3) to embarrass the regime, publicize the motivation and behavior of the ruling elite, and attempt to force responsibility for human rights abuses. They have maintained visibility in the social media but as more traditional users, publishing statements and videos, not as competent hackers.

Though not sufficient, cyberspace can provide a fruitful complementary domain of conflict, and there are both benefits and drawbacks of non-state actors as a part of a conflict strategy. Most of the benefits revolve around the low entry costs for small-scale attacks and the asymmetric advantages for attackers. Due to their lean organizational structure global effects can be achieved faster, cheaper and without limitations due to geography (Mulvenon and Rattray 2012a, 127–128). They are also easier recruited due to the lack of geographical constraints, little risk for life and health (at least outside the conflict zone), and the somewhat limited skills required. By the use of political online message boards and social media, hackers are able to recruit a large, ideologically motivated force at short notice. The flexible structure results in lacking potential for maintaining organization and united strategy as we see in the anti-regime faction. It makes it harder to maintain human capital, and there are fewer opportunities for educating "the next generation". This reduces the embedded human capital and creates dependence on existing members' competence. In the end this reduces organizational memory, and causes loss of information (Mulvenon and Rattray 2012b, 164). Due to the lack of coercive control and punishment, cost of deflection, and lack of centralized leadership, online social movements have weaknesses embedded in its structure. We see all these tendencies in the Syrian case.

The anti-regime faction is weaker and gains less attention as they lack unity and cooperation. SEA has a greater focus on training, and we have seen in the case study that they are rather synchronized. The research also indicates that SEA uses many resources on training, and even established a hacker school to train volunteers. In the case of the anti-regime, this is

only recorded as provided by foreign assistance. The case study has shown that the guerrilla tactics are successful in the case of the SEA, that enjoys the most resources and organization, but the lack of coordination and unity hampers the work of the opposition. Equal to real world guerrilla warfare, cyber guerrillas depend on some level of organization to maximize the benefits of the strategy. Without this, their efforts are limited to that of vandals or hooligans voicing their opinions as individuals instead of as a force. However, it must be pointed out that this tentative conclusion only based on one case. It is likely that the SEA and the Assad regime cooperate to an unknown extent and, depending on the level, the comparison between SEA and the anti-regime non-state actors may be skewed. However, both the theoretical and empirical foundation demonstrates that SEA uses guerrilla tactics. The comparison is therefore right, as they both use the asymmetrical tactic and has no formal bonds with a government. If the links between the regime and SEA are as the opposition claims, the appropriate mirage would be the African guerrillas in Africa during the Cold War, enjoying support from the two super powers but with no formal links.

As wee see, all the assumptions find some support in the Syrian case. It is clear that the non-state actors are greatly involved in the cybered aspects of the conflict. They, to some extent, qualify as cyber guerrillas. Their attacks seem to indicate a subversive goal, based in the spread of strategic narratives and a relative soft power balance. However, an element of hard power is also found as surveillance and online impersonations are introduced. These tactics are based in fear, not perceived legitimacy in the recipient. We also see diverging levels of success in the campaigns launched by the non-state actors at both sides of the conflict. But, as pointed out at several occasions through this research project, any conclusions made here are indicative instead of definitive as the field is young and the empirical record is short. It therefore does not seek to make conclusions beyond the immediate empirical record collected for this thesis. Regardless, the support for the assumptions may indicate a potential framework for the growing presence of non-state actors in cyberspace. We will now evaluate to what extent Syria qualify as a cybered soft war.

Is it a soft war in Syrian cyberspace?

This thesis has attempted to answer the: "*Why and how does non-state actors use cyberspace in modern conflict?*" To do so, it first had to establish that non-state actors use cyberspace in a conflict situation. It was foundational belief that was confirmed by the Syrian case, though few past studies focus on this kind of actors. Secondly, the case study asked why they use their scant resources in a domain unable to determine the course of a conflict. An indicative answer is that the goal is to subvert the opposition, be it pro- or anti-regime, but a conclusive answer cannot be given at the present time. What is more clear is that they, due to their relative power, use guerrilla tactics to push an agenda of soft wars; meaning strategic narratives to influence the soft power balance. The case study also shows that the domain favors an offensive strategy. Attackers spearhead attacks by choosing the time and place, thus forcing defense "everywhere". If the aim is subversion, the number of potential targets is also close to endless. SEA illustrates this element with their global scope on potential victims. Attacker also "set the agenda" by deciding the scale and type of attack. These groups can therefore be valuable in a revolutionary setting to demonstrate cause, fellow supporters, and undermine the authority of the regime/ opposition by humiliation and delegitimizing tactics. This case study therefore clearly indicates that non-state actors use guerrilla tactics and can, like fleas on a dog, hurt the more powerful enemy. This gives them credence as actors on the political stage, and strengthens the importance of this thesis' focus point. The Syrian actors have the means and a favorable environment, but this does not guarantee a successful use. The case study shows that in Syria we see that the non-state actors with regime allegiance have a higher empirical record and level of attention, but the materialization of desired effects are questionable. The case study, lastly, demonstrated the importance of resources and organization also in this domain. It therefore indicates that cyberspace is not neutral, where actors' position is only determined by innovation. Instead one party to the conflict sets the parameter for operations and are able to limit both the reach and scope of the other. Traditional measurements of strength apply to this domain as the SEA dominates the current cyber conflict in Syria.

Today, in Syria we see "cyber-armies", both pro- and anti regime, waging organized (dis-) information campaigns in cyberspace. As this thesis have shown, both parties actively uses social media to "sell their story" to the domestic and global audience. Going beyond social media, they actively use hacking as a tool in conflict and manipulate how events are

perceived. These groups sabotage, persecute and spy on each other and perceived supporters by hacking accounts, defacing websites, and manipulating social media outlets. Pushing an agenda of subversion, it is more conflictual the past cybered conflicts in for example Estonia and Georgia. Their actions mirror traditional disinformation and propaganda campaigns, but the focus on the soft power balance resembles that of information warfare. The case study shows that the non-state actors and state actors both use the Internet to allot disinformation, shape public opinion, spread propaganda, and delegitimize opponent. The hackers voice their objections, create attention for their opinions, and build fear among the opposition. Additionally, cyberspace is shown to enable both extensive intelligence gathering and a new domain for the "battle of narrative". Attention and influence is the life-blood of any movement, and as we have seen in this thesis the groups actively use cyberspace to form public opinion and the political agenda. However they only have limited, if any, physical consequences. The actors also have little control over effects, and cannot therefore be classified as powerful. This work concludes that the campaigns analyzed resemble more sabotage, vandalism and guerrilla warfare than traditional military action.

If the will and the mind of the opponent is the target, then "softer tactics" are placed central stage. By framing attitudes and perceptions, battles can be won. This has been referred to as soft wars. We clearly see that the actions of the actors studied here are aimed at selling their version of reality to shape how events are interpreted. This is not a new phenomenon. As "representatives of the people", "liberators" or "protectors", combatants have justified why they engage in the violent spiral that is war. Through their narratives they build a version of reality, which is done to engage support, secure position and build legitimacy. They are engaged in what can be named "soft war". They manipulate perceptions to an instrumental and political manner, and though not directly violent it targets the actual conflict. Thus they use guerrilla tactics to build a momentum and secure their place as "fish in the sea". Additionally cyberspace acts as a force multiplier by allowing the non-state actors to create confusion and attack the enemy's center of gravity. This case study thus concludes that cyberspace merely provides a new domain to do what has always been done, but its scope and low entry barrier allows for the entry of non-state actors to an extent not seen before. By focusing on cybered conflicts in a soft war perspective, why non-state actors chose to focus their scant resources in this domain is explained. The risks are lesser than in real world conflict, while the rewards may be great. Combining Rid's arguments with Arreguin-Toft's findings thus allows for an analytical framework to explain why Syrian non-state actors chose

to spend resources in cyberspace despite its lack of lethal effects. By using cyberspace as a political and instrumental domain to shape perceptions, combating non-state actors may strengthen their position in real world conflicts.

Attention is attention; cyber attacks become one way of being noticed among the many causes and groups in today's interconnected world. Like protests, signature campaigns, vandalism and use of traditional media, cyber attacks are becoming a way to show defiance. You only need a few accomplished members, not all must be able to use the "printing press" (develop the software) as long as there are some that can help spread the newspapers/ malware to the public. Removal of websites is comparable to censorship of newspapers and libraries in attempts to limit inputs and shape public opinion. Attacks undertaken may allow control of information, which in turn can hamper decision-making and/ or manipulate the behavior of opposing parties. The actions of the groups studied here can also be compared to how students or oppositions vandalize in real world conflicts to spread their message or gain attention of the public. SEA is especially accomplished in this type of work, and they have understood that attacking news media is an excellent way of gaining their attention. Not only do they get the attention of whoever visits a given webpage, but also by the mediums covering the story. In sum they force their way onto the front page. We therefore see clear indications that the Syrian cyber actors use this domain to influence domestic and international politics.

The empirical record supports that cyber power and soft war allows for a holistic analysis of non-state actors similar to the past research into states. Cyberspace may force the behavior of others, either by preventative attacks like DDoS, which complicates coordination and organization, or psychologically by recruitment and sustainability of existing supporters. The attacks aim to create a perception of strength, and in the case of SEA result in more international attention than a group of its magnitude is entitled. The second face of cyber power, as envisioned by Nye (2010), is not found in the Syrian conflict. This is in hindsight logical, as we have seen that non-state actors have limited possibility to exclude potential strategies beyond DDoS (first face of cyberpower). The third face of cyberpower however is also present in the Syrian conflict, and it can be argued that the line between the second and third face is blurred in the Syrian case. As seen in the beginning of the thesis, the second face entailed exclusion of strategies while the third meant the change of preferences so some strategies were never considered. We see a growth in use of surveillance, which in turn

excludes potential strategies of adversaries. But it also may make the potential costs so great that the strategy is never considered. The identification and punishment of opposition members captured online have expansive effects, as potential anti-regime individuals will reconsider using software vulnerable for infiltration. As SEA is able to manipulate and infiltrate without the victims' knowledge, it is likely that the anti-regime groups will "self-censor" out of fear of retaliation.

In sum this leads the opposition to miss out on the benefits of cyberspace seen in Egypt and Tunisia, possibly indicating a change in the "social media revolutions" sometimes accredited as the catalyzer for the Arab Spring. The truth to this claim is at best debated, but what is seen in the Syrian case is that cyberspace is manipulated and used against the opposition. Online impersonations, large-scale surveillance, and rumors of information sharing with the regime's security services, most likely limits the effectiveness of the cyber domain for the opposition, again unlike the Egyptian and Tunisian case. As we have seen there is also accusations claiming that the regime only allows social media sites as a way to entrap opposition members. This allows us to at least question if the Arab Spring's most famous tool is now turned against them? Contrary to common belief, in Syria it does not necessarily provide a neutral domain but instead yet another battlefield.

The case study has demonstrated that in a conflict over hearts and minds creating a perceived winner is vital. Cyber actors therefore matter as they can be used to build perceptions. When building a narrative, common tactics are the presentation of imminent threats and catastrophic potential consequences, reports of attacks and abuse, vilification of the opponent, and declare opposition as the only viable position (Nissen 2013). All of these are used by the actors in the Syrian cybered conflict, and after two years this pattern in clearly identifiable. There is an ongoing battle of perception and narrative between the parties, both targeting the population and the international audience(see also Nissen 2013). The argumentation either builds on the legitimate right to uphold law and peace in the sovereign territory, or the right to rebel against unjust leaders. The enemy is either described as foreign-backed criminals without respect for law and order, or as maniac regime run by corruption and oppression. Both use video and photos actively to present stories and evidence supporting their narrative. Common is also proof of inhumane behavior at the hand of the other, thus legitimizing the struggle for survival of the sender and use of extraordinary means. By claiming that the opposition is supported and lead by foreign powers, the SEA may undermine the revolution's legitimacy as

"representatives of the people". Secondly, its' cyber operations build a perception that the regime is still strong and should be feared. Thirdly, by spreading accusations of human rights violations at the hand of the opposition the regime can undermine their moral authority as protesters against a despotic regime. The potential for hacking user accounts in ICT and social media, and to give damaging information to the regime; may prevent activists for using these channels and thus limiting their potential for coordination and influence. In total, these factors may contribute to regime recruitment or passivity in the citizenry but obviously these effects are next to impossible to measure at the current time and are therefore simply speculations. Syria becomes therefore the last chapter in a trend prominent over the last 15-20 years: the increased focus on the informational parts of warfare as seen in Yugoslavia, Afghanistan, Libya, Iraq and Somalia (Nissen 2013, 89). Due to technological advancements this also happens with unprecedented scope and speed.

Final thoughts

Kosovo was described as the first War on the Internet (Denning 1999, 1), but this thesis has shown the development of cybered conflicts is moving rapidly. We see the multiple types of conflicts that exist today[107], and cyberspace's role varies depending on the circumstances. In many non-internationalized conflicts, the effects of cyberspace are minimal in the Clausewitzian sense. It is yet to be demonstrated that non-state actors can have disruptive effects on a state by cyber operations (Geiss 2013, 5). However the use of cyberspace as an integrated part of strategy increases the importance of the domain, and may in the greatest consequence have violent ramifications. Several cases studies show the effectiveness of the Internet for activism, especially in combination with other types of mass media and a clear political agenda. There should be therefore no surprise that the Internet has become a popular tool among activists from around the globe with all types of motivations. To quote Denning (1999):

> It facilitates activities such as educating the public and media, raising money, forming coalitions across geographical boundaries, distributing petitions and action alerts, and planning and coordinating events on a regional or international level.

Manipulating ICT allows for diffusion of command, targeting of opposing narratives and "custom-made" narratives targeted at the different groups of recipient. When traditional media dominated, there were only a few reporters present when an event took place. Today, any individual with a smart-phone can be a reporter and therefore create propaganda, secure communication, gather intelligence, and apply for funds. Whine (1999, 238) therefore concludes that ICT has assisted in a shift of non-state organization from hierarchical to hydra-headed networks, similar to what Joseph Nye's dubbed "diffusion of power" . This shift, with a growing number of actors and parties to a conflict, is clearly present in this case study. It finds that the structure of cyberspace both encourage and facilitates the presence and involvement of non-state actors. Thus the strategy of a coordinated narrative may be complicated, but the potential for alterations and supportive "proof" of one's point of view is much greater. In sum, It is therefore clear that ICT is becoming a battleground for the "hearts of the minds", where competing narratives seeks to sway the targeted population.

[107] E.g. low-intensity armed conflicts between organized armed groups in failed-State scenarios like Somalia, "traditional types of civil war" like the ongoing, armed conflict in Syria, "internationalized" scenarios like in Afghanistan (Quote from Geiss, 2013).

Joseph Nye Jr. states that future conflict will be characterized by "states will remain the dominant actors on the world stage, but they will find the stage far more crowded and difficult to control" (quoted in Mulvenon and Rattray 2012a, xii). As the literature referred illustrates, former studies have tended to focus on state actors in cyberspace, or non-state actors in traditional forms of conflict. However non-state actors are becoming a force and require scrutiny. The combination of the non-lethal nature of cyberspace, the great demand of resources to yield significant effects, and the low cost of entry adds up to the conclusions that non-state actors will utilize cyberspace. However, it is likely that it will be utilized as a medium to drum up support, engaging in the battle of the narrative, and soft wars as in this case study and not in the hope of yielding determining effects in real wars. However, this field of study is to young to make any conclusive recommendations concerning a whole area of research. It therefore does not seek to make conclusions beyond the immediate empirical record collected for this thesis. Regardless, the support for the assumptions may indicate a potential framework for the growing presence of non-state actors in cyberspace. But much research is needed before any theory can be developed. However, this thesis demonstrates that many insights to real world conflicts can be transferred to those in cyberspace. It simply offers a new domain and does not fundamentally alter the ways of conflict.

Bibliography

Al Jazeera, The Stream Team. 2013. “New Report Exposes Digital Front of Syria’s Civil War.” Al Jazeera. http://america.aljazeera.com/watch/shows/the-stream/the-stream-officialblog/2013/12/25/new-report-exposesdigitalfrontofsyriascivilwar.html.

Alexander L. George, and Andrew Bennet. 2004. Case Studies and Theory Development in the Social Sciences. Cambridge: MIT Press.

Applegate, Scott. 2011. “Cybermilitias and Political Hackers—Use of Irregular Forces in Cyberwarfare.” https://www.academia.edu/1098232/Cyber_Militias_and_Political_Hackers_-_Use_of_Irregular_Forces_in_Cyber_Warfare (June 12, 2013).

Arquilla, John, and David Ronfeldt. 1995. “Cyberwar and Netwar: New Modes, Old Concepts, of Conflict.” RAND Review. http://www.rand.org/pubs/periodicals/rand-review/issues/RRR-fall95-cyber/cyberwar.html.

Arreguin-Toft, Ivan. 2001. “How the Weak Win Wars: a Theory of Asymmetric Conflict.” International security 26(1): 93–128.

Assir, Serene. 2013. “Syrian Electronic Army Battles for Public Opinion through Cyber Attacks.” Agence France Presse. http://www.huffingtonpost.com/2013/06/09/syrian-electronic-army-battles-public-opinion_n_3412843.html.

Baiazy, Amjad. 2012. “Syrian Cyber Wars.” UK London. MediaPolicy report. http://www.mediapolicy.org/2012/06/syrias-cyber-wars/.

Bennet, Andrew. 2004. “Chapter 2: Case Study Methods: Design, Use and Comparative Advantage.” In I Detlef F. Sprinz & Yael Wolinsky-Nahmias, Eds. Models, Numbers and Cases, Methods for Studying International Relations, Michigan: University of Michigan Press.

Bennett-Smith, Meredith. 2012. “Anonymous Declares War On Syrian Government Websites In Retaliation For Internet Blackout.” The Huffington Post. http://www.huffingtonpost.com/2012/11/30/anonymous-declares-war-syrian-government-websites_n_2218447.html.

Berger, George. 2013. “Is Clausewitz or Sun Tzu More Relevant to Contemporary War?” e-irinfo. http://www.e-ir.info/2013/04/03/is-clausewitz-or-sun-tzu-more-relevant-to-understanding-contemporary-war-2/.

Bogart, Nicole. 2013. “Propaganda Vs. Self-censorshiå: Syria’s Virtual Civil War.” Global News. http://globalnews.ca/news/809766/propaganda-vs-self-censorship-syrias-virtual-civil-war/.

Boone, Jed. 2013. “Syrian Electronic Army Revealed: Anonymous Hacks SEA Website, Dumps Data.” Global Post. http://www.globalpost.com/dispatches/globalpost-blogs/the-grid/syrian-electronic-army-revealed-anonymous-hacks-sea-website-dum.

Boot, Max. 2013. Invisible Armies. New York: Liveright Publishing.

Bradsbury, David. 2013. “Information Warfare: a Battle Waged in Public.” Computer Fraud and Security. http://www.sciencedirect.com/science/article/pii/S1361372313700551.

Brumfield, Ben. 2012. “Computer Spyware Is Newest Weapon in Syrian Conflict.” CNN. http://edition.cnn.com/2012/02/17/tech/web/computer-virus-syria/.

Carr, Jeffery. 2011. Inside Cyberwarfare. 2nd ed. USA: O’Reilly Media Inc.

Casebeer, William D., and James A. Russel. 2005. “Storytelling and Terrorism: Towards a Comprehensive Conter-narrative Strategy.” Strategic insights, Center for Contemporary Conflict at the Naval Postgraduate School 4(3).

Castells, Manuel. 1997. The Information Age: Economy, Society and Culture Volume III: The Power of Identity. Malden, Ma: Blackwell Publishers.

Cavelty, Myriam Dunn. 2013. “Cyber Security.” In Alan Collins Contemporary Security Studies 3rd Edition, UK: Oxford University Press.

CENTCOM. “About U.S. Central Command (CENTCOM).” http://www.centcom.mil/about-u-s-central-command-centcom.html (April 22, 2014).

Chalabi, Mona. 2014. “Syrian Electronic Army’s War on the Web: Interactive Timeline.” The Guardian. http://www.theguardian.com/world/interactive/2013/sep/03/syrian-electronic-army-war-web-timeline (October 1, 2014).

CIA Factbook. “Syria.” CIA Factbook. https://www.cia.gov/library/publications/the-world-factbook/geos/sy.html (January 26, 2014).

Cook, Thomas D., and Donald T. Cambell. 1979. Quasi-experimentation : Design & Analysis Issues for Field Settings. Boston: Houghton Mifflin Co.

Cyber Security Dictionary. 2012. “SCADA.” Cyber Security Dictionary. http://www.projectauditors.com/Dictionary2/1.8/index.php/term/,62555c9cae535a6f68555cad5d56.xhtml (April 22, 2014).

Deibert, Ronald. 2013. Waging the Cyber War in Syria. Electronic Frontier Foundation. https://www.eff.org/mention/ronald-deibert-waging-cyber-war-syria.

Denning, Dorothy E. 1999. “Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.” In The Internet and International Systems: Information Technology and American Foreign Policy Decision Making, San Francisco: Nautilus Institute. http://www.iwar.org.uk/cyberterror/resources/denning.htm.

Dickinson, Elizabeth. 2009. “IN BOX: A Bright Shining Slogan How ‘Hearts and Minds’ Came to Be.” Foreign Policy. http://www.foreignpolicy.com/articles/2009/08/13/a_bright_shining_slogan.

Diesen, Sverre. 2013. “The Usefulness of Military Force as a Tool of Statecraft.” Presented at the Oslo, University of Oslo.

Eisenhardt, K.M. 1989. “Building Theories from Case Study Research.” Academy of

Management Review 14(4): 532–50.

Findley, Michael G., and Joseph K. Young. 2007. “Fighting Fire with Fire? How (Not) to Neutralize an Insurgency.” Civil Wars 9(4): 378–401.

Fisher, Max, and Jared Keller. 2011. “Syria’s Digital Counter-Revolutionaries.” The Atlantic. http://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/ (November 20, 2013).

Fitzpatrick, Alex. 2012. “Social Media Becoming Online Battlefield in Syria.” Mashable. http://mashable.com/2012/08/09/social-media-syria/.

Franceschi-Bicchierai, Lorenzo. 2013. “Syrian Electronic Army Attacks Linked to Obama’s Mentions of Syria.” Mashable. http://mashable.com/2013/10/09/syrian-electronic-army-obama-cyberattacks/ (April 15, 2014).

Freedom House. 2013. Freedom on the Net: Syria. Freedom House. Freedom on the net 2013. http://www.freedomhouse.org/report/freedom-net/2013/syria#.U3nVj16FG4o.

Furlow, R. Bennet, and H.L. Goodall Jr. 2011. “The War If Ideas and the Battle of Narratives: a Comparison of Extremis Storytelling Structures.” Cultural Studies, Critical Methodologies 11(215).

Galperin, Eva, and Morgan Marquis-Boire. 2012. “New Trojan Spread Over Skype as Cat and Mouse Game Between Syrian Activists and Pro-Syrian-Government Hackers Continues.” Electronic Frontier Foundation. https://www.eff.org/deeplinks/2012/06/darkshades-rat-and-syrian-malware (November 2, 2014).

Garrett, R. Kelly. 2006. “Protest in an Information Society: A Review of Literature on Social Movements and New ICTs.” Information, Communication and Society 9(2): 202–24.

Gary King, Robert O. Keohane, and Sidney Verba. 1994. Designing Social Inquiry: Scientific Inference in Qualitative Research. Princton University Press.

Geers, Kenneth. 2011. “Strategic Cyber Security.”

Geiss, Robin. 2013. “Cyber Warfare: Implications for Non-international Armed Conflicts.” International Law studies (INT’L L.STUD) 627(89).

Gerring, John. 2004. “What Is a Case Study and What Is It Good For?” American Political Science Review 98(2): 341–54.

———. 2005. “Causation: A Unified Framework for the Social Sciences.” Journal of Theoretical Politics 17(2): 163–98.

———. 2007. Case Study Research. Principles and Practices. Cambridge: Cambridge University Press.

Gitlin, Todd. 2003. The Whole World Is Watching. Berkley adn LA, California: University of Berkley Press.

Goodman, Seymour E., Jessica C. Kirk, and Megan H. Kirk. 2007. “Cyberspace as a Medium for Terrorists.” Technological forecasting and social change 74(2): 193–210.

Grange, David L. 2000. “Asymmetric Warfare: Old Method, New Concern.” National Strategy Forum Review.

Hackers News Bulletin. 2013. “Syria: Ministry of Health Website Hacked by Anonghost.” http://hackersnewsbulletin.com/2013/06/syria-ministry-of-health-website-hacked-by-anonghost-team.html.

Bøe-Hansen, Ola. 2010. “Taliban Og ISAFs Propagandakrig- Kampen Om Den Mest Overbevisende Historien.” Institutt for forsvarsstudier Norwegian Institute for Defence Studies. Masterthesis.

———. 2012. “Media Og Fellesoperasjoner.” In Eldar Berli (red.) Innblikk I Fellesoperasjoner, Forsvarets Stabsskole Skriftserie,.

Harding, Luke, and Charles Arthur. 2013. “Syrian Electronic Army: Assad’s Cyber Warriors.” The Guardian. http://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background (October 3, 2013).

Holden. 2013. Measuring the Media Impact of Hacktivists. Analysis Intelligence. http://analysisintelligence.com/tag/syrian-electronic-army/ (October 3, 2014).

Hunker, Jeffrey. 2010. “Cyberwar and Cyber Power – Issues for a NATO Doctrine.” Research paper NATO Defense College, no 62.

Hutchinson, W., and M. Warren. 2001. “Principles of Information Warfare.” Journal of Information Warfare,Volume 1(1).

ICANN. “Welcome to ICANN.” Internet Corporation for Assigned Names and Numbers (ICANN). https://www.icann.org/en/about/welcome (April 22, 2014).

International Telecommunication Union. 2013. ICT Facts and Figures 2013. International Telecommunication Union. Times series by country, Core indicators on access to and use of ICT by households and individuals. http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (September 4, 2014).

———. 2014. Fixed (wired) Broadban Subscription Per 100 Inhabitants Syria. Geneve, Sveits: International Telecommunication Union. ITU’s ICT-EYE. http://www.itu.int/net4/itu-d/icteye/ (March 5, 2014).

Janssen, Cory. “ISP.” Technopedia. http://www.techopedia.com/definition/2510/internet-service-provider-isp (April 22, 2014).

Jowett, Garth S., and Victoria J. O’Donnel. 1999. Propaganda and Persuasion. 3rd ed. SAGE publications.

Kaldor, Mary. 2013. “In Defense of New Wars.” Stability 2(1)(4): 1–16.

Kallberg, Jan, and Bhavani Thuraisingham. 2013. “From Cyber Terrorism to State Actors’

Covert Cyber Operations." Strategic Intelligence Management: National Security Imperatives and Information and Communications Technologies 1(229-233).

Kalyanaraman, S. 2003. "Conceptualisations of Guerrilla Warfare." Strategic Analysis 27(2).

Khamis, Sahar. 2013. "Media and Arab Transitions The Role of the Media in Arab Transitions: How 'Cyberactivism' Is Revolutionising the Political and Communication Landscapes." IEMed Mediterranean Yearbook 2013.

Khamis, Sahar, Paul B. Gold, and Kathrine Vaughn. 2012. "Beyond Egypt's 'Facebook Revolution' and Syria's 'YouTube Uprising:' Comparing Political Contexts, Actors and Communication Strategies." Arab Media & Society (15). http://www.digitalislam.eu/article.do?articleId=7440.

———. 2014. "Propaganda in Egypt and Syria's 'Cyberwars': Contexts, Actors, Tools and Tactics." In The Oxford Handbook of Propaganda Studies, by Jonathan Auerbach and Russ Castronovo (eds.), Oxford University Press.

Kaarbo, Juliet, and Ryan K. Beasley. 1999. "A Practical Guide to the Comparativ Case Study Method in Political Psychology." Political Psychology 20(2): 369–91.

Langø, Hans-Inge. 2013a. "Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security." NUPI Working Paper 820.

———. 2013b. "The Limits of Compulsory Cyber Power: Assessing Ecological Potential and Restraints in the Digital Domain." NUPI Working Paper, Norwegian Institute of International Affairs 819.

Lasswell, Harold. 1972. Propaganda Technique in the World War. Garland Publisher.

Leuprecht, Christian, Todd Hataley, Sophia Moskalenko, and Clark Mccaule. 2010. "Containing the Narrative: Strategy and Tactics in Countering the Storyline of Global Jihad." Journal of policing, Intelligence and Counter Terrorism 5(1): 42–57.

Levy, Jack S. 2008. "Case Studies: Types, Designs, and Logics of Inference." Conflict managment and peace science 25(1): 1–18.

Lewis, James A. 2010. "Thresholds for Cyberwar." Center for Strategic and International Studies.

Lijphart, A. 1971. "Comparative Politics and the Comparative Method." American Political Science Review 65(September): 682–93.

Lynch, Marc, Deen Freelon, and Sean Aday. 2014. Syria's Socially Mediated Civil War. United States Institute for Peace. Blogs and Bullets. UIPS.Org.

Maliukevičius, Nerijus. 2006. "Geopolitics and Information Warfare: Russia's Approach." Lithuanian Annual Strategic Review 2006: 121–47.

Mavhunga, Clapperton. 2008. The Glass Fortress: Zimbabwe's Cyber-Guerrilla Warfare. http://concernedafricascholars.org/bulletin/issue80/mavhunga/.

McKenzie Jr., Kenneth F. 2001. “The Rise of Asymmetric Threats: Priorities for Defense Planning.” In NAT’L DEF. UNIV., QDR 2001 STRATEGY-DRIVEN CHOICES FOR AMERICA’S SECURITY by Michele A. Flournoy (ed.),.

Moses, Jonathon W., and Torbjørn L. Knutsen. 2007. Ways of Knowing. Basingstoke: Palgrave McMillian.

Mulvenon, Dr. James, and Dr. Gregory Rattray. 2012a. Addressing Cyber Instability. Cyber Conflict Studies Association.

———. 2012b. “Introduction.” In Dr. James Mulenon and Dr. Gregory Rattray (eds.) Addressing Cyber Instability, Cyber conflict studies association.

National Post Wire Services. 2013. “Dow Jones Plummets, Then Recovers after Fake AP Tweet of Explosions at the White House.” Financial Post. http://business.financialpost.com/2013/04/23/dow-jones-plummets-then-recovers-after-fake-ap-tweet-of-explosions-at-the-white-house/ (April 5, 2014).

Neal, Ryan W. 2013. “FBI Adds Syrian Electronic Army To Wanted List; Supporters Of Hacker Collective Will Be Regarded As Terrorists.” Ibtimes. http://www.ibtimes.com/fbi-adds-syrian-electronic-army-wanted-list-supporters-hacker-collective-will-be-regarded-terrorists (September 4, 2014).

Nissen, Thomas Elkjer. 2013. “Chapter 6: The Ever Changing Narrative of Conflict – How the Role of War Narratives Changes from Mobilizing for the Battle of Perceptions to Influencing Histor.” In Carsten Jenssen (ed). Democracy Managers, Copenhagen: Royal Danish Defense College, 73–89. http://forsvaret.dk/FAK/eng/publications/Documents/Democracy%20Managers.pdf.

Noman, Helmi. 2011a. Syrian Electronic Army: Disruptive Attacks and Hyped Targets. Information Warfare Monitor. http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/.

———. 2011b. The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army. The Information Warfare Monitor.

Nye, Joseph S. 2004. Soft Power: The Means to Success in World Politics. USA: Public Affairs.

———. 2010. “Cyber Power.” Harvard Kennedy Belief center for Science and International Affairs. From the author’s forthcoming book, The Future of Power in the 21st Century, Public Affairs Press, 2011.

O´Hagan, Jancita. 2013. “War 2.0: An Analytical Framework.” Australian Journal of International Affairs 67(5): 555–69.

Ottis, Rain. 2010. “From Pitchforks to Laptops: Volunteers in Cyber Conflicts.” In Estonia: Talinn: CCD COE, 98–109.

Oxford Dictionary Online. 2014. “Non-state Actor.” Oxford Dictionary. http://www.oxforddictionaries.com/definition/english/non-state-actor (January 2,

2014).

Pearlman, Wendy, and Kathleen G. Cunningham. 2012. “Nonstate Actors, Fragmentation, and Conflict Processes.” Journal of Conflict Resolution 56(February): 3–15.

Perlroth, Nicole. 2013. “Hunting for Syrian Hackers’ Chain of Command.” NY Times. http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html.

Peterson, Andrea. 2014. “Syria Hit with a Near Nationwide Internet Outage for Seven Plus Hours.” Washington Post. http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/20/syria-hit-with-a-near-nationwide-internet-outage/.

Phelan, Jessica. 2012. “OpSyria: Anonymous Declares Cyberwar on Syrian Government for Taking Syria Offline.” Global Post. http://www.globalpost.com/dispatch/news/regions/middle-east/syria/121130/opsyria-anonymous-declares-cyberwar-syrian-government.

Preston, Jennifer. 2011. “Seeking to Disrupt Protesters, Syria Cracks Down on Social Media.” NY Times. http://www.nytimes.com/2011/05/23/world/middleeast/23facebook.html?_r=2&.

Reporters without Borders. 2013. Enemies of the Internet: Special Edition: Surveilance: Syria. Reporters without borders. http://surveillance.rsf.org/en/syria/ (September 4, 2014).

Rid, Thomas. 2013. Cyber War Will Not Take Place. UK London: Hurst and Company.

Ringdal, Kristen. 2007. Enhet Og Mangfold – Samfunnsvitenskapelig Forskning Og Kvantitativ Metode’. 2nd ed. Bergen: Fagbokforlaget.

Rogan, Eugene. 2011. The Arabs: a History. 2nd ed. USA: NY: Basic Books.

Ronfeldt, David. 1998. The Zapatista Social Netwar in Mexico. Santa Monica, California: RAND.

Rouse, Margaret. 2009. “RAT (remote Access Trojan).” Search Security. http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan (March 20, 2014).

Ruus, Kertu. 2008. “Cyber War I: Estonia Attacked from Russia.” European Affairs 9(1-2). http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html.

Salhani, Justin. 2013. “In Syria, the Cyberwar Intensifies.” C4ISR Journal (January/ February issue). http://www.defensenews.com/article/20130118/C4ISR01/301180018/In-Syria-Cyberwar-Intensifies.

Sammut, Tim, and Mike Schiffman. 2014. “SQL Injection.” Cisco Security. http://www.cisco.com/web/about/security/intelligence/sql_injection.html (March 20, 2014).

Sauter, Molly. 2013. “Distributed Denial of Service Actions and the Challenge of Civil

Disobedience on the Internet." Center for Civic Media, MIT. Submitted to the Program in Comparative Media Studies/Writing on May 17, 2013 in Partial Fulfillment of the Requirements for the Degree of Master of Science in Comparative Media Studies.

Scott-Railton, John, and Morgan Marquis-Boire. 2013. A Call to Harm: New Malware Attacks Target the Syrian Opposition. Canada: Toronto: The Citizens Lab, Munk School of Global Affairs, University of Torronto.

SEA. 2014. "Syrian Electronic Army Official Website." http://www.sea.sy/index/en (April 4, 2014).

SECDEV Foundation. 2012. Flash Note : Syrian Cyber Watch. SECDEV foundation. Ad-Hoc Reports. http://secdev-foundation.org/recent-publications/ and https://docs.google.com/file/d/0B-szos-lFcMSaWpnUGJRZlpQYzg/edit.

———. 2013a. Flash Note: Syria's Hacker War. Canada: SECDEV foundation. http://www.technewsworld.com/story/78904.html.

———. 2013b. SYRIAN ELECTRONIC ARMY LEAKS: CYBER ESPIONAGE & HACKTIVISM AS A WEAPON IN THE SYRIAN CIVIL WAR. SECDEV foundation. Flash Note Syria. https://docs.google.com/file/d/0B-szos-lFcMSQVpFbWc5VU1UV1U/edit.

Shehabat, Ahmad. 2012. "The Social Media Cyberwar: The Unforlding Events of the Syrian Revolution 2011." The Global Media Journal- Australian Edition 6(2).

Shehadi, Nadim. 2013. "Revolution or Civil War? The Battle of Narratives in Syria." OpenDemocracy. http://www.opendemocracy.net/opensecurity/nadim-shehadi/revolution-or-civil-war-battle-of-narratives-in-syria (July 5, 2014).

Sheldon, John B. 2013. "The Rise of Cyber Power." In John Baylis, James Wirtz and Colin Gray (eds). Strategy in the Contemporary World 4th Edition, UK: Oxford University Press.

Siegel, Robert, and Morgan Marquis-Boire. 2013. "In Syria, Conflict In Cyberspace Complements Ground War." http://www.npr.org/2013/12/31/258699442/in-syria-conflict-in-cyberspace-complements-ground-war?sc=tw.

Sigholm, J. 2013. "Non-State Actors in Cyberspace Operations." Journal of MIlitary Studies 4(1).

Soy, Susan K. 1997. "The Case Study as a Research Method, Uses and Users of Information." https://www.ischool.utexas.edu/~ssoy/usesusers/l391d1b.htm.

Stalinsky, Steven, and R. Sosnow. 2013. Syrian Electronic Army Uses Social Media – Twitter, YouTube, Facebook, Instagram, Google+, Pinterest, Smartphone Apps – To Communicate, Spread News Of Its Hacks And Its Mission, And Recruit Volunteers. The Middle East Media Research Institute. http://www.memri.org/report/en/0/0/0/0/0/0/7357.htm.

Stout, Mark. 2009. "In Search of Salafi Jihadist Strategic Thought: Mining the Words of the

Terrorists." Studies in Conflict & Terrorism 32(10): 876–92.

Sumey, Miranda. 2013. The Syrian Question. USA: Washington DC: The George Washington University, Cyber Security Policy and Research Institute. Online commentary. http://www.cspri.seas.gwu.edu/1/post/2013/09/the-syrian-question.html.

T Chen, and J.M. Robert. 2004. "The Evolution of Viruses and Worms." In W. Chen (Ed.) Statistical Methods in Computer Security, New York: Marcel Dekker.

Toor, Amar. 2011. "Anonymous and Tunisia: A New Cyber Warfare?" Switched, HuffingtonPost Tech. http://www.switched.com/2011/01/29/anonymous-and-tunisia-a-new-cyber-warfare/.

Wallace, David A., and Shane R. Reeves. 2013. "Non-State Armed Groups and Technology: The Humanitarian Tragedy at Our Doorstep?" 3 U. Miami Nat. Sec. & Law of Armed Conflict J. Summer 2013(forthcomming). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295078.

Whine, Michael. 1999. "Cyberspace- a New Medium for Communication, Command and Control by Extremists." Studies in Conflict & Terrorism 22(3): 231–45.

York, Jillian C. 2011. "Syria's Twitter Spambots." The Guardian. http://www.theguardian.com/commentisfree/2011/apr/21/syria-twitter-spambots-pro-revolution.

Zalman, Amy. 2010. "A Battle of Narratives:narrative as an Influence Factor in Information Operations." IO Journal 2(3).

Appendix

The complete record of the empirical data collected is submitted to the University of Oslo's, Institute of Political Science Administration together with this thesis on the 23rd of May 2014. It is collected in a excel document which is too big for printing in a Word format. It is therefore delivered on a memory stick, one copy, in accordance with UiO rules. Additional copies can be requested to the author at vivi.ringnes@gmail.com.