Turun yliopisto
University of Turku

CYBER ATTACK CAMPAIGNS IN POLITICAL CONFLICTS

A case study of Anonymous hacktivists' campaign against ISIS

Master´s Thesis
in Information Systems Science

Author:
Otto Sulin

Supervisor:
Jonna Järveläinen

16.02.2018
Turku

Table of Contents

List of figures

List of tables

Abbreviations

AQI = Al-Qaida in Iraq
C2 = Command and Control
CCDCOE = (NATO) Cooperative Cyber Defense Centre of Excellence
DDoS = Distributed Denial of Service (attack)
DoS = Denial of Service (attack)
FTP = File Transfer Protocol. A simple protocol for moving files between hosts.
JN = Jabat al-Nusra
UN = United Nations
HUMINT = Human Intelligence
ISIS = Islamic State in Iraq and Syria; also ISIL, Islamic State in Iraq and Levant
ICS = Industrial Control System
IMPACT = International Multilateral Partnership Against Cyber Threats
IP = Internet Protocol
IRC = Internet Relay Chat
LOAC = Law of Armed Conflict
OPSEC = Operational Security
SCADA = Supervisory Control And Data Acquisition [System]
SFTP = Secure File Transfer Protocol
SIGINT = Signals Intelligence
SSH = Secure Shell. A remote connection protocol that uses strong encryption.
SQL = Structured Query Language. A database programming language.
XSS = Cross-site Scripting (attack)

1 INTRODUCTION

1.1 Internet, the new frontier of conflicts

Cyber warfare can be considered at the same time as an old and new topic. In academic research the topic of cyber warfare has had active discussion already for more than 25 years. Despite that cyber operations saw the light of day as a method for political gain only a decade ago. This was the case of Estonia in 2007, when after moving an old Soviet war memorial, the Bronze Statue, to a new site the Estonian infrastructure got under a massive cyber attack consisting mainly of Distributed Denial of Service (DDoS) that made government websites, banking services and media websites unavailable. What makes this cyber warfare and not just a casual cyber attack, are the facts that it was clearly politically and not financially motivated and had many ties to motivations of Kremlin. Germany, Israel, Finland and Slovenia along with NATO CERT team had to help Estonia that was not able handle the attack by itself (Kozlowski, 2014).

World Wide Web was born on 6 August 1991, thus 2005 serves as a good mid-point in the journey of Internet as we know it so far. On 26.07.2017 Google Scholar service found 59 200 articles discussing cyber warfare. That shows us that at least the academia has a growing interest in the topic. Another dimension to the importance of the topic is growth of Internet usage. The number of Internet users has grown from December 2005 1018 million users to December 2015 3366 million users (Internet World Statistics, 2015). The reason why this fact is important is clear: our lives are more and more on the Internet, and where people lead their lives there is an arena for using political power.

"War is not merely a political act, but also a real political instrument, a continuation of political commerce, a carrying out of the same by other means" (von Clausewitz, 1832) is an often-cited definition of war. Clausewitz's statement could interpreted to say that means of war are just an extension to politics and a means to exercise political power. The cyberspace, or Internet, is just another dimension to this as are air, land and sea – the older domains of war. Internet provides alluring possibilities for conducting military and intelligence operations. Cyber operations can also be very cost-efficient as anything can be conducted from homeland without setting any physical infrastructure or personnel near the target, Internet bandwidth and salaries being the main costs. They can even be out-sourced to commercial or political hacker groups to maintain deniability. (Borghard & Lonergan, 2016)

As we can see, Internet is becoming the new field of extending political power, and an increasingly relevant one. But there's more. The open and quite anonymous nature of

Internet brings us a distinct difference compared to the other fields of war: anyone can participate without the others knowing who is participating.

1.2 Scientific motivation for this study

Cyber-based conflicts are likely to evolve as use of Internet evolves in our society. Firstly, the more and more pervasive digitalization all around gives the topic a growing relevance as everything from our refrigerator to social life is on the Internet (Rohan, 2017). Thus, the potential impact of a cyber war on citizens' daily lives is growing fast, even though they would be far away from the organizations waging the war, as we are increasingly adopting cloud services that might be physically located on the other side of the planet. (Gartner, 2017) As Internet becomes a larger part of our lives, it is only logical that our political conflicts also move to this growing dimension. Studying these conflicts with case studies will shed light on the smaller details of how Internet can be used as platform for political influence and conflicts.

The modern history in international politics has been guided by Westphalian sovereignty, which states that nations have power over their territory and domestic affairs on the principle of non-interference from external powers (Kissinger, 2014). During the last 40 years we've seen emergence of dozens of powerful paramilitary political groups that have significant state-like capabilities for violence on all continents (Nash, 1998). In the context of this study, most interesting are powerful terrorist organizations that wield significant power because of the asymmetrical nature of their methods. Examples of these could be FARC in Colombia, HAMAS in Palestine and Boko Haram in Northern Africa region (US State Department, 2016). After World War II non-state actors have claimed more importance in international politics, making international relations more complicated and sometimes even greatly influenced by non-state actors (DeLuca, 2013). More and more we are seeing this phenomenon in the cyberspace too, like the case of Syrian Electronic Army that is an active political group wreaking havoc on the Internet (Al-Rawi, 2014).

This leads to the second motivation for this study: in this case study, non-state actors conduct the entire political conflict. Denning (2010) concluded that cyber conflicts are mostly conducted by non-state actors. By the time of this study, ISIS isn't recognized as a state by the UN but listed as a terrorist organization (United Nations, 2013). Anonymous on the other hand is neither a state nor a terrorist organization, but a loosely organized hacktivist collective. This setting makes the object of the study one with very new features: a conflict in cyberspace with two resourceful non-state actors.

Thirdly and lastly, the data available for the study is very unique. There are many studies (Geers et al., 2014) about cyber attacks that have allegedly been conducted by a

nation-state all around the globe that cover in detail cyber attacks by states such as China, United States, United Kingdom and Russia. A large body of research on non-state actor cyber attacks can also be found. But only rarely do studies have a major part of the data available for the research – at least for the academia openly to publish about it. Cyber attacks are conducted all the time, but rarely does there exist a dataset publicly available for anyone to analyze it.

This study uses publicly available data, data that actually is giving a very broad picture of the conflicts and cyber attacks from one side of the war, in this case, the side of Anonymous. The data for this study is completely open like the very nature of Internet itself. On the other hand, like on the Internet, also a lot of relevant information is either hidden or at least it is borderline impossible to get it. The latter doesn't invalidate the study in any way, and it will be discussed later on, but should just be accepted as a natural limitation. In the very essence of cyber attacks and operations, it is hard to see the entire picture (Hunker et al., 2008, 5).

1.3 General overview of the study

The aim of this study is to produce a modern view on methods of cyber operations in cyber-based conflicts – and on the blurry concept of cyber warfare. This study will evaluate the cyber attack methods that were available by the time of this study to be used.

The research questions of this study are the following:

- How do political conflicts escalate in cyberspace to cyber attacks or warfare?
    - What are the phases of a cyberspace-based conflict?
    - What are the actors in cyber conflicts and attacks?
    - When can a conflict in the cyberspace be called cyber warfare or terrorism?
- How do cyber attack campaigns proceed in a political conflict?
    - How and what kind of cyber attacks can be used in a political conflict?

The first part of the literature review will delve into the idea of cyber-based conflict. The first section seeks to provide a high-level understanding of politically motivated conflicts in the cyberspace and introduce the key concepts that are building blocks of cyber-based conflicts that escalate to attacks or warfare. To provide structure to empirical analysis of a conflict, this study aims to dissect the concrete building blocks of cyber-based conflict. Legal issues are important in international conflicts and they will be discussed as well, even though legal interpretations are not the focus of this study.

The second part of literature review will focus on the actual methods available for the actors to use in operations in the cyberspace. As with conventional military and physical weapons, detailed methods and tactics can be outlined. Details of cyber attack methods will be analyzed to some extent to provide a decent basis for analyzing cyber attacks. Focus is on the process of cyber attacks and how it relates to the developing political conflict.

The main objective is to form a clear picture of how two non-state actors can use cyber attack methods in their conflict. Using the constructed theory of methods of cyber conflict models acquired from the literature review this study goes on to analyze the methods that hacktivist group Anonymous used in its campaign #OpParis, a revenge campaign against ISIS after the Paris attacks on November 13th 2016. This study will analyze that what were methods used by Anonymous compared to the frameworks derived from current scientific literature and expert opinions. The material will be reflected also from the point of view of the entire conflict and its timeline – what was the sequence of events? How did the conflict and methods escalate?

2 POLITICAL CONFLICTS AND WARFARE IN THE CYBERSPACE

This chapter aims to briefly present the concept of having a social or political conflict – or even a war conducted through methods that are considered to be cyber attacks. First section will deal with political and social conflicts in general, and it will present a sequential model of a cyber conflict. After defining cyber conflict development, the literature review will focus on the actors of conflicts in the cyberspace. Lastly, the concept of cyber warfare and relevant existing legislation will be briefly discussed for clarity.

2.1 Conflicts in the Cyberspace

There are many points of view for a cyber conflict. You can look it at the point of participants or from pure definition, but the point of view chosen for this study is longitudinal, sequential analysis of the events in a cyber conflict. In this section, a staged model of events will be presented to give an observer a framework for following a conflict as a sequence of events. Definitions for conflicts as political phenomena will explored as well.

To put a frame to the conflict, we must first define the boundaries of activity we are observing – in this context the keyword that must be defined is "cyberspace". Kuehl (2009) defined it such that *"…cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information communication technologies."* In the current context, we'll define a cyber conflict to be situated, physically or otherwise, as stated in the previous chapter on definition. To put it shortly, a cyber conflict happens in the man-made information networks and around the people and devices connected to the networks. Here terms "cyberspace-based" and "cyber" as used interchangeably.

2.1.1 Perspectives on different types of conflicts

It can always be questioned whether a conflict is political or social. According to Pruitt and Kim (2014), *"**Social conflict** is the struggle for agency or power in society. Social conflict or group conflict occurs when two or more actors oppose each other in social interaction, reciprocally exerting social power in an effort to attain scarce or incompatible goals and prevent the opponent from attaining them. It is a social relationship wherein the action is oriented intentionally for carrying out the actor's own will against*

the resistance of other party or parties." The viewpoint of social context is very relevant in cyberspace as not all of the actors are nation-states and thus not all actors view the conflict as situation for policy, but maybe just items to act on. Hacktivist groups, like Anonymous, can be geographically dispersed and actually from around the globe, but might rally collective for a cause and take action through the Internet.

Theories on social conflict take varying angles when defining social conflict. According to Rummel (1976) *"By definition, social is intentionally taking into account other selves, power is a capability to produce effects, and social power is an intentionally directed capability to produce effects through another person. Social conflict is then the confrontation of social powers. What does this view imply? First, social conflict is exclusively an aspect of social power. To understand such conflict we must deal at the level of social powers and their dialectics, as power or conflict social theorists have done."* Rummel goes on to define the underlying motivation as conflict of interests, interests being non-altruistic needs like power and financial needs.

As can be noticed from the example of Bronze Statue issue, political conflicts can expand to cyberspace as well. According to Heidelberg Institute for International Conflict Research, "***A political conflict*** *is a positional difference regarding values relevant to a society - the conflict items - between at least two decisive and directly involved actors, which is being carried out using observable and interrelated conflict means that lie beyond established regulatory procedures and threaten a core state function or the order of international law, or hold out the prospect to do so."* (HIIK, 2011).

As a political conflict can manifest itself anywhere we can reasonably deduct that even pure cyber conflicts may exist, but if the other participant or several of them are non-state actors it can questioned whether the conflict is social or political or both.

In this study, the question of sociological context for how cyber conflicts should viewed is not discussed further, but left as an open question for every individual conflict as something on observer should be cognizant of. In the chapter "Actors in Cyber Conflicts", this study shed more light on the actors of cyberspace that is the defining factor for how the conflict should be observed, as it is the actors that will affect whether it is sensible to view a conflict as either political or social conflict – cyberspace is only the arena.

2.1.2 Analyzing conflicts

Analyzing conflicts has been subject to various theories, which vary from psychological, social, economical, political to pure mathematics. Deutsch et al. (2011) summarized the following eight analytical approaches to conflict theory (adapted):

- Differential equations; using a system of equations to model the conflict.

- Decision theory / conflict theory; analyzing utility maximization of agents.
- Game theory; analyzing two or more agents' choices of different alternatives to maximize payoff.
- Bargaining theory; observing conflict as negotiation between two or more parties.
- Uncertainty; taking into account uncertainty of each action and event in a conflict.
- Stability theory; analyzing the conflict based on an equilibrium and deviations from it.
- Action-reaction models; focus on interaction among agents in a conflict.
- Organization theory; attempting to predict behavior inside an organization.

Of these eight analytic approaches, this study focuses on what is called action-reaction models. The reason for this choice is that to be able to analyze different phases, and possible interaction within phases, this study evaluates different action-reaction models that can clearly show the actions and sequential development qualities of a conflict in cyberspace.

An example of such model could be the phased model Kadende-Kaiser et al. (2003) presented, which had been adapted from Sriram & Wermester (2003):

Potential Conflict	There are factors that cause stress between the actors, which may be for example economic or social.
Gestation of Conflict	Growing amount of factors cause situation to develop towards conflict.
Trigger / Mobilization of Conflict	Building tensions, threats or even confrontations between parties.
Conflict / Escalation	Violence that causes for example casualties, human rights abuse or similar.
Postconflict	End to conflict activities, risk of new conflict remains.

Table 1 Phases of conflict (Sriram & Wermester, 2003)

Kadende-Kaiser et al. (2003) also point out that conflicts between two parties are not static and time-bound. Conflicts also vary in time, intensity and duration. They also point out that phased models allow analysis of a conflict without fixing oneself to some predetermined chronological and view conflict with more open approach. This why this study explores existing phased models, limiting to the ones focused in modeling cyberspace-based conflicts.

2.2 Evaluation of existing cyber conflict models

To date, there are not many attempts to model cyber conflicts from the pure cyber conflict perspective, especially from phased perspective, which Grant et al. (2015) also concluded in their research on offensive cyber operations models. No model reviewed by Grant et al. included the potential political aspect of cyber attacks. Neither does it seem that any single has been accepted as the standard model, as observed from the literature reviewed for this study. This may be because the field of study is still developing and no model has consistently proven useful in analyzing different cyber attack campaigns or conflicts.

2.2.1 Cyber Early Warning Model

One such model is Carr's (2011) "A Cyber Early Warning Model" that is a 5-stage model of how cyber conflicts develop. The model in Figure 1 consists of five parts that are presented in a linear sequence, but they are not necessarily linear in reality and have significant overlapping and iterative features.

Figure 1 A Cyber Early Warning Model (Carr 2011)

Latent tensions are any tensions, grudges or animosity between groups that might be nation-state or non-state actors. Referring to the Estonia case presented in the introduction, the tensions could be the political tensions between Estonia and Russia, and their difficult relationship because of the past in Soviet Union (Carr, 2011). In this study, tensions are related to political tensions between any two groups.

Cyber reconnaissance are the steps that groups take against each other prior to starting a hostile activity to discover vulnerabilities from target infrastructure. This information can be used to make the attacks more efficient (Carr, 2011). Reconnaissance consists of gathering information related to networks (IP addresses, domain names), hosts (operating

system versions, running services), persons using the target systems (phone numbers, personal information) and security policies (security appliances used, password complexity requirements). These pieces of information will be used to find a weak spot in the target system or organization (Sanghvi & Dahiya, 2013). Cyber reconnaissance will be discussed with more details in the next chapter.

Initiating events are the events that make either one or more parties take action as a threshold is reached. In the Estonia case, the removal of the Bronze Statue was the event (Carr, 2011). Similar events in history have happened in many instances in global politics, for example archduke Franz Ferdinand's assassination started the chain of events that lead to World War I (Stone, 1966).

Cyber mobilization is a process of massing force against decisive points (Elkus, 2009). In this stage the actor uses publicity and political rhetoric to incite people to join the cause. Cyber mobilization has already been effective in politics; the event known as Arab Spring that began from Tunis in December 2010 that lead to riots and governments being overthrown in several Arab nations would not have been possible without cyber mobilization. In cyber mobilization different information and communication technologies are used to rally the masses. In Arab Spring focus was especially on social media (Allagui & Kuebler, 2011).

Cyber attacks are the wide spectrum of operations that parties can carry against each other over the means of networks and computer devices. For brevity, discussion on definition of cyber attacks will be left short here and will be discussed with detail in the next chapter.

Carr's model is a high-level model of different modes that a conflict can have in cyberspace. It can be questioned and studied if the model would be any different for non-cyberspace context and answer would likely be no, but that answer doesn't downplay the relevance of the model for analyzing cyber-based conflicts. If the model is assumed as foremostly iterative the order of the conflict's different activities is not crucial. If not, then the question should be raised if "Cyber recon" is truly before "Initiating events". Carr is making an assumption that the aggressive party of the conflict does proactively prepare for a conflict in cyberspace and gathers information accordingly. This obviously may or may not be true; the aggressive party could start its reconnaissance operations after the initiating event has triggered the response.

2.2.2 Ventre's model

Ventre (2011) proposes the following model in his book Cyberwar and Information Warfare:

- **Intelligence phase**; cyber intelligence can be divided to two categories:

    - Technical intelligence, that comprises of all technical information-gathering methods, e.g. document metadata.
    - Human intelligence, which is the human side of data collection from the Internet. An example of this would manual collection of personal details of key target personnel from social medias sites like LinkedIn and Twitter.
- **The planning phase and generating forces**; the act of planning the attack thoroughly.
- **The conduct phase**; the operational part of attack. The conduct phase consists of the attack operations itself, supporting forces and ensuring anonymity.

This model is seemingly similar to Carr's (2011) Cyber Early Warning model. The difference is that political tensions are left out and what in Carr's model were called "Cyber mobilization" and "Cyber reconnaissance" have been combined to a single "The planning phase and generating forces" phase. Such simplification might be considered justified if thought from the perspective of an army, which is moving methodically step by step towards the attacks. However, it can subject to critique in context of other actors than formal nation-state armies.

2.2.3 Discussion on evaluated models

Regarding the current literature on cyber conflict models two conclusions can be made. Firstly, field of research is still developing; only few models that have both properties of being phased conflict modes and being focused on the cyber aspects. Only few models were available which makes sense as relatively small amount of research data to date exist to support such research. Secondly, all models are fairly similar consisting of similar building blocks which have only been grouped differently.

Carr's (2011) model is more detailed than Ventre's (2011) model. Carr's Cyber Early Warning Model with its latent tensions, cyber reconnaissance, initiating events, cyber mobilization and cyber attacks is clear in its structure. The different phases included in the model should be observable separately from a cyber conflict. The model provides a good base for analyzing the high-level developments of the conflict as well as diving deeper into each phase as needed.

2.3 Actors in Cyber Conflicts

All conflicts need participants to become a reality and so do cyber conflicts too. The distinctive feature of cyber conflicts is that the picture of who is participating in the conflict will never be certain and clear. (Wheeler & Larsen 2003, 68) The possibilities of masquerading as someone or something else are endless on the Internet.

To press the point, a network log data might show that cyber attacks are coming from China, but nobody knows if the attackers are actually Chinese or are they just trying to disappear in the flood of cyber attacks originating from China. In this example, China could provide a sound narrative for many law enforcement specialists who very likely will not press further after seeing the origin, knowing that it would be either very hard or impossible to find the attacker. Using countries with reputation for corrupt officials and weak justice system is a very rational choice on the part of attacker who wishes to remain anonymous.

2.3.1 Non-state actors

A significant feature of cyber conflicts is the emergence and strong presence of various non-state actors. This has been brought up by many researchers and authors (Carr, 2011; Andress & Winterfield, 2014; Kallberg & Thuraisingham, 2013). In the current literature, a non-state cyber actor may be an individual, corporation, organized crime group, terrorist, autonomous agent or other similar actor (Brown, 2016).

Even though the reality of participants of a cyber conflict remains uncertain, there are certain categories and types of actors present in the space. Sigholm (2013) from Swedish National Defense College categorized different actors in the cyberspace. Table 2 includes the main non-state actors in cyber conflicts as categorized by Sigholm, and it's very comprehensive at that. Despite all these actors being first and foremostly non-state, in reality it might be a thin red line between being a state operation or not, let alone an observer being able to make such distinction. It also relevant to point out, that not all of the actors in Table 2 are politically or socially motivated – most are not.

Actor	Motivation	Target	Method
Ordinary citizens	None (or weak)	Any	Indirect
Script kiddies	Curiosity, thrills, ego	Individuals, companies, governments	Previously written scripts and tools
Hacktivists	Political or social change	Decision makers or innocent victims	Protests via web page defacements or DDoS attacks
Black-hat hackers	Ego, personal animosity, economic gain	Any	Malware, viruses, vulnerability exploits
White-hat hackers	Idealism, creativity, respect for the law	Any	Penetration testing, patching
Grey-hat hackers	Ambiguous	Any	Varying
Patriot hackers	Patriotism	Adversaries of own nation-state	DDoS attacks, defacements
Cyber insiders	Financial gain, revenge, grievance	Employer	Social engineering, backdoors, manipulation
Cyber terrorists	Political or social change	Innocent victims	Computer-based violence or destruction
Malware authors	Economic gain, ego, personal animosity	Any	Vulnerability exploits
Cyber scammers	Financial gain	Individuals, small companies	Social engineering
Organized cyber criminals	Financial gain	Individuals, companies	Malware for fraud, identity theft, DDoS for blackmail
Corporations	Financial gain	ICT-based systems and infrastructures (private or public)	Range of techniques for attack or influence operations
Cyber espionage agents	Financial and political gain	Individuals, companies, governments	Range of techniques to obtain information
Cyber militias	Patriotism, professional development	Adversaries of own nation-state	Based on group capabilities

Table 2 Main non-state actors in cyber conflict (Sigholm 2013)

By looking at Sigholm's (2013) categorization of different types of main non-state actors and their motivations, we can dissect the following actors to be politically or socially motivated non-state actors:

- Ordinary citizens
- Hacktivists
- Patriot hackers
- Cyber terrorists
- Cyber espionage agents
- Cyber militias.

Regarding these actors, it could said that lines between them are more or less blurry – what is the real difference between hacktivists and patriot hackers, or when is an actor hacktivist or a black hat hacker? That would depend on the perspective of an individual hacker or their self-defined group mentality. The difference of cyber militia and cyber terrorist might depend on the perspective of the observer. This discussion must be done on case by case basis and this study relies on Sigholm's categorization. While "ordinary citizen" does not need further definition, the other politically motivated non-state actors may not be as clear.

Hacktivism as a phenomenon could be defined as a combination of hacking and activism, and is a form political action done collectively (Denning, 2001). Hacking then is about gaining access to computers and networks without permission (Cresswell, 2010). Hacktivists use hacking methods for political ends (Illia, 2003).

Patriot hackers are hackers that are motivated by interests of a nation and they conduct cyber attacks against parties that are seen as enemies of their nation. For the nation, patriotic hackers are a useful resource as the nation can easily deny being part of the effort and they can effortlessly wave away any efforts of cross-border police action to stop the hacking. Cases of patriotic hacking have been noted at least in Russia and China. The problematic side of patriot hackers is that the nation may not be able to stop them from hacking when it would be in their political interests, as was noticed in the aftermath of 2001 Hainan collision of Chinese and American fighter jets. Eventually Chinese government had to arrest their own citizens to stop the hacking. Patriot hacker groups are referred to as 'cyber militia', which is discussed later in this chapter. (Singer & Friedman, 2014)

Cyber terrorists are not easy to define, as term 'terrorist' itself has vivid political and legal connotations. Even international community is struggling with the definition. Whether a political actor attacking armed forces of another nation can be called a terrorist, or when does freedom fighter become a terrorist are still seen as ambiguous questions (Ruby, 2012). United Nations General Assembly declared in a Resolution in 1994 (United Nations, 1994):

"Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them."

Suffice to say, cyber terrorists are terrorists using cyber methods. Cyber terrorism is discussed in detail later in this chapter for better clarity.

To define 'cyber espionage agents', the concept of espionage must be first discussed. According to Oxford Dictionary (2017) espionage is *"the practice of spying or of using spies, typically by governments to obtain political and military information"*. In the context of this study, let cyber espionage be defined as espionage carried over cyber reconnaissance and attack methods, which will be explored more closely in later chapters.

Cyber militia can be defined to be patriot hackers acting as a group. Hollis (2015) discusses uses of cyber militia in detail in his "Cyberwar case study: Georgia 2008", discussing how cyber militia can be used by nation-states for various political gains. According to Hollis (2015), cyber militia can be organized clandestinely by a nation-state before or during a crisis to conduct actions in such way that the cyber militia can cause an effective with their group power but the underlying, supporting nation-state stays hidden or at least in a status where they can deny their support.

2.3.2 State actors

State actors are discussed here briefly as comparison to non-state actors to give a broader picture of cyberspace actors. Moreover, it may be hard or impossible to discern when an attacker group is actually a state or a non-state group, which is why one should always take into account all possibilities. While the study by Sigholm (2013) discussed earlier brought a dozen different non-state actors into discussion, it doesn't mean governments were not active in advancing their political motives on the Internet. A number of governments have begun their official cyber security programs during last couple of years (Luiijf et. al, 2013). Offensive capabilities are not advertised openly and programs' public disclosure is focused on defensive security. The capabilities are combined from research of Besseling et al. (2013) and from a research by Wall Street Journal (Valentino-Devries & Yadron, 2015).

In the study by Valentino-Devries & Yadron (2015), all countries referred to surveillance capabilities and goals in some form. Lithuania, Japan, Romania and Uganda were not included in the study of Valentino-Devries & Yadron, but they hadn't included any references to offensive capabilities in the other study.

To summarize the lengthy table (Appendix 1):

- 67 countries seem to have some level of offensive cyber capabilities.
- 70 % of countries (47) use purchased software, and a smaller part of 46 % use software developed in the country (31). Some of these used both developed and purchased software.
- Main usage is for surveillance, and though in many countries there are indications of usage against activists and opposition, main goal seems to be enhancing police operations against criminals.

Comprehensive studies about nation-state cyber capabilities seem to be lacking and any study coming public would immediately be more or less outdated as the capabilities develop fast in the current political climate. For this reason, Table 6 in Appendix 1 is in this context only for illustrative purposes – it could be stated that governments do not only plan for defensive but also for offensive cyber capabilities. Without doubt governments are increasingly active actors in the cyberspace.

2.4 Cyber warfare and terrorism in political conflicts

2.4.1 Defining cyber warfare

Cyber warfare is a widely discussed topic with varying opinions. The topic seems to have its hawks and doves, as the saying goes in politics. Both researchers and politicians tend to deviate towards either end of the spectrum. Some of these opinions may be due to lack of understanding of cyberspace. (Dombrowski & Demchak, 2014). Also, the question of existence of cyber warfare can also be viewed from the point of view of current legislation.

Several publications, such as book “There Will Be Cyberwar” (Stiennon, 2015), have pushed towards the more hyped position. “There’s an arms race in cyberspace, and a massively exploding new cyber-industrial complex that serves it.”, said Deibert & Rohozinski (2011) along similar lines in their column called “The New Cyber Military Industrial-Complex”. These points of view are likely moving the discussion to a more radical position, giving politicians and decision makers a sense of urgency and danger. Such language may give a non-technical person quite radical picture about the landscape of political cyber attacks and what can be achieved with them.

On the other hand, there are analysts and researchers on the dovish position. For example, “Cyber War Will Not Take Place” (Rid, 2012) and another article titled “The Fog of Cyberwar: Why the Threat Doesn’t Live Up to the Hype” (Maness & Valeriano, 2012)

argue that cyber war has not, is not currently and will never happen. Rid (2012) goes on to argue that cyber war is rather what has previously been characterized as sabotage, espionage and subversion. Neither does Rid find that any single cyber offence to date could be interpreted as act of war, referring both to von Clausewitz's definition and the legal definition, which both could be summarized as inflicting casualties or significant physical damage to the opponent. Another factor pushing the cyber war hype to unreasonable extent in United States, a prolific source of writing on cyber war, might be the large base of military contractors that see cyber war as potential new business area (Deibert & Rohozinski, 2011).

By looking at the titles mentioned previously one can easily conclude the polarity of the discussion; subject matter experts, researchers and politicians are taking exact obvious stances on the topic. Thirdly, there is the point of view of law, which previously mentioned mostly ignore by rather taking a practitioner standpoint. Regarding legal point of view, two differing stances should be clarified:

- Current legislation is up to date.
- Current legislation is not up to date, and should be revised to take into account latest developments in technology.

More specifically, as this study does not concern any country but all countries in the world, this question is about international legislation. Most international legislation covering warfare has been written right after Second World War, which is why the second argument against the existing legislation may be valid, as technology has progressed with rapid speed after the laws were written.

However, whether the current international legislation is suitable or not, is a question for another study and it won't be discussed further. This study takes current international law as is, using what can be considered modern and common interpretations of it.

2.4.2 Definition of cyber warfare

While previous chapter shed light on all the actors and seemingly wide range of political activity on the Internet, the definition and discussion on the actual cyber warfare is still lacking. In this chapter goal is to provide a concise definition and understanding of the concept of expanding warfare activities to the cyber context.

With the concept of cyber warfare we enter the difficult discussion on defining terms that have very critical legal and political repercussions. The legal aspect will be postponed until next chapter and now the focus is on the more practical point of view. Both politics and academia have produced a number of definitions, and below are presented two concise definitions:

- “Cyber Warfare is cyber attacks that are authorized by state actors against cyber infrastructure in conjuntion [sic] with government campaign” (East-West Institute, 2014).
- "’Cyber warfare’ means actions by a nation/state to penetrate another nation's computers and networks for purposes of causing damage or disruption” (Government of South Africa, 2011).

A more classical definition was offered by Carl von Clausewitz (1832) in *On War*. As interpreted by Rid (2012), Clausewitz (1832) argues that a war has three clear characteristics:

- Violent. “War therefore is an act of violence to compel our opponent to fulfil our will”. Violent and forceful actions are always needed in a war.
- Instrumental. “War is always a serious means for a serious object.” War is always means to an end.
- Political. “The war of a community—of whole nations and particularly of civilised [sic] nations—always starts from a political condition, and is called forth by a political motive. It is therefore a political act. - - War is a mere continuation of politics by other means.” A war is never an isolated event but a piece in a larger puzzle.

This widely cited piece from Carl von Clausewitz seems to make it at the same time possible but also difficult to state that a cyber attack – or a campaign of attacks is actually war. While the two latter points are easily achieved with cyber attacks – it only has to have political goals – the first one is tricky. A strict interpretation of violence would mean that cyber attacks would have to cause physical harm, which cannot be excluded as a possibility, but no such events can be found recorded and analyzed from the current scientific literature. Another angle to address this issue would be to ask: can non-physical harm causing cyber attacks be interpreted as acts of war? To this question, there are no simple answers.

2.4.3 Legal status of cyber warfare and attacks

Currently no comprehensive international legal form governs or defines how cyber arms and attacks relate to previous legislation. The only concept close to an international agreement on the issue is the Council of Europe Convention on Cybercrime which is ratified also in some countries outside of the European Union, namely by United States, Canada,

Japan and South Africa (Council of Europe, 2001). This convention is a source of definitions for cybercrime and forms of international cooperation regarding cybercrime, as most of the largest and most developed economies are members to the convention.

The main questions lies in whether a cyber attack is considered as ”use of force” as it’s defined in the United Nations Charter in Article 2(4), which leads us to the topic of Law of Armed Conflict. In legal context, military conflicts are generally divided to two topical categories: 1) *jus ad bellum*, meaning the justification for going to war, and 2) *jus in bello*, meaning how wars are fought, as governed by the conventions of Geneva and Hague and the United Nations Charter is the basis for most of the current legislation of warfare. The Law of Armed Conflict (LOAC) applies only to situations where Geneva conventions apply, i.e. there are lawful combatants that are under the protection of the Geneva Convention rules of handling enemy combatants (Andress & Winterfield, 2011). The question of who is and when a lawful combatant is very difficult in cyber-based conflicts as the combatants might not be recognizable or located in military controlled facilities or subject to other proxy-enabled recognition as they might be civilians ordered to do military cyber operations. The last-mentioned situation is a very real legal and practical problem as many countries are challenged with building their war-time cyber troops while at the same time not being able to maintain the same personnel in peacetime, which leads to the conclusion that conscripting cyber warfare capable personnel might be the only option (Brenner & Clarke, 2011).

Experts from the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) have proposed a legal framework in documentation called the Tallinn Manual (CCDCOE, 2013). The Tallinn Manual is so far the only comprehensive suggestion of legal base for cyber warfare and conflicts, but it’s currently not in a form of legislation but only a proposal. Below are presented the key ideas of the Tallinn Manual, paraphrasing Andress & Winterfield (2011) and the Tallinn Manual, as agreed by the majority of International Group of Experts involved in the process:

- States may not knowingly allow their cyber infrastructure to be used for cyber attacks against other countries
- States may be held responsible, even though the attacks were not committed by state agencies but by other groups in direction of the state.
- Use of force is prohibited in cyberspace as it is physical environments. Threshold for interpreting act as use of force is such action that causes harm to people or damages objects.
- Merely causing inconvenience doesn’t qualify as use of force.
- States may respond to use of force with countermeasures that do not exceed those directed towards it.

- A State victim an “armed” cyber attack may answer with either cyber or kinetic force. Cyber operations resulting in significant damage to property or loss of life qualifies as an armed attack.
- Victim State may respond in self-defense to attacks by non-state actors, and the victim State may even be allowed to use force against non-state actors located in another State.
- An entirely cyber-based conflict qualifies as an “armed conflict”, thus protecting both combatants and other individuals by existing international legislation.
- In a cyber-based armed conflict, individuals responsible of ordering actions may be held responsible for war crimes.
- Civilians conducting cyber operations during an armed conflict may be interpreted as lawful combatants.
- Attacks against civilians and civil infrastructure are not entirely prohibited during an armed conflict.
- Cyber attacks against civilians are war crimes if they injure or are likely to do so. It is also unlawful to use cyber operations to spread terror among civilians.
- All cyber weapons must be subject to legal review before use on the battlefield.
- Cyber attacks must be directed at lawful targets that may not unintentionally target civilians.
- Cyber operations must be used instead of conventional weaponry if civilian damage can be averted by feasible cyber operations.
- Existing humanitarian laws apply fully regarding cyber operations.

Despite the work in the Tallinn Manual process and the political activity on the Internet, international law still lacks legislation regarding cyber warfare. But as can be seen from the previous summary of the key points of Tallinn Manual, there is a broad, existing legislation regarding war and use of force, which can be fairly easily applied to this new kind of use of force if needed.

However, in reality making any cyber attacks be considered as ‘international armed conflict’ is not as trivial. Even classifying state-actor attacks as ‘armed conflict’ is difficult, with sometimes small group’s actions is even more as they should be qualified as ‘armed group’. This situation may change as the attacks may become more destructive as societies become more dependent on information technology (Schmitt, 2012).

2.4.4 Cyber terrorism from legal perspective

If war can be conducted on the Internet, so can terrorism too. Pollitt (1998) defines cyber terrorism as *"the premeditated, politically motivated attack against information, computer systems, and data which results in violence against non-combatant targets by sub national groups and clandestine agents"*. Comparing to the previously mentioned issue of how do cyber attacks relate to the UN Charter definition of use of force, cyber terrorism has much clearer picture. States, especially the military superpowers, prefer to have the legislation more or less unclear on definitions to give them the freedom to provide a narrative that fits their political agendas. But regarding terrorism, objectives are much more aligned towards clear definitions and viable models of cooperation, as terrorism isn't likely an issue arising strictly inside country borders but much more likely to have international elements and actors included. Thus, there is a clear need for cooperation.

A variety of legal agreements and documentation on terrorism exists. According to Manap, Taji and Tehrani (2013) there are 17 UN conventions that relate to cyber terrorism (Appendix 2). The previous authors also remind that despite all the legislation, only one UN body specializes in dealing with cyber attacks which is the International Telecommunications Union (ITU). Backed by ITU, IMPACT (International Multilateral Partnership against Cyber Threats) began its operation in Malaysia in March 2009, as world's first global partnership against cyber threats, acting as a center for anti-cyber terrorism intelligence and helping all of its 191 members in large-scale cyber terrorism threats against global financial systems, power grids, nuclear plants and air traffic control systems. According to their website, the organization is *"- - the first comprehensive public-private partnership against cyber threats, ITU-IMPACT serves as a politically neutral global platform which brings together governments of the world, industry, academia, international organisations, and think tanks to enhance the global community's capabilities in dealing with cyber threats."* (Manap M., Taji H. and Tehrani P., 2013 & IMPACT-Alliance, 2016).

Thus we can conclude that cyber attacks, performed by non-state actors that don't have a clandestine backing of a geopolitical power could face substantial political action from UN or nations taking actions based UN interpretations, as the legal framework for taking actions clearly exists. So far the world hasn't seen a situation where the Security Council or other similar body has taken action after a non-state cyber terrorism action.

3 CYBER ATTACK OPERATIONS

Whereas the previous chapter explored the socio-political context of cyber conflicts and warfare, this chapter delves to the actual real-world methods that are available for actors to use. First, we'll look at models of targeted cyber attacks. Next, intelligence gathering and attack methods will be examined on a practical level, after which the growing field of information operations will be elaborated.

The goal of this chapter is to provide definitions for different types of cyber attack methods. These definitions and categorizations will be used later to analyze the material of this study and label the used methods accordingly.

In this chapter, terms cyber weapon and cyber attack method will be used interchangeable. This is due to current literature having very varying use of terminology. The preference of this study is to use the broader term "cyber attack method", as the word weapon also has a legal connotation and linguistically may not be understood to also encompass psychological methods.

Similarly, in literature words reconnaissance and intelligence might be used quite freely and interchangeably. In this study 'intelligence' is preferred, but 'reconnaissance' might be used if original text referred to had used this word instead.

3.1 Cyber Operations Models

The Tallinn Manual Section 5 defines cyber weapons such that *" - - cyber weapons are cyber means of warfare that are by design, use or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack - - "* (CCDCOE, 2013).

The discussion of the different models of cyber attacks isn't linear as there isn't only one model. Existing literature isn't elaborating the idea of multifaceted attacks that have either multiple goals or uses supporting vectors with the main attack method. Example of this would be an attack aiming at data exfiltration by exploiting security vulnerabilities, but supports the attack with a DDoS that acts as a smokescreen to mask the real intention. Nevertheless, existing literature is teeming with descriptions of cyber attack models and a review of them is covered in this chapter.

This section draws heavily on research done by Grant et al. (2015). Grant et al. did an extensive review of existing models of offensive cyber operations, which will be used as basis in this chapter. In their review seven different models were evaluated. Some models were rejected from the review because they did not meet the quality criteria used by Grant

et al. The research and resulting model by Grant et al. was chosen as the basis for operational level analysis for this study because the goal is to analyze cyber conflicts in a sequential, process like manner, which also was a requirement for Grant et al. Also, their review was a meta-analysis of several modern models can be considered as broad-sighted because of that.

The models analyzed to form the canonical model were analyzed against five factors:

- Context; for example 'crime' or 'warfare'.
- Basis; for example 'literature', 'case studies' or 'hackers' writings'
- Attacker; 'lone' or 'group'
- DoS; included in the model or not.
- Temporal aspects; included in the model or not.

All the analyzed models used a linear process in depicting the offensive cyber operation. The models were formalized using Structured Analysis and Design Technique (SADT) notation, and were brought into a canonical model by rational reconstruction. Below is an overview of the model as represented by in 'Comparing Models of Offensive Cyber Operations' (Grant et al., 2015).

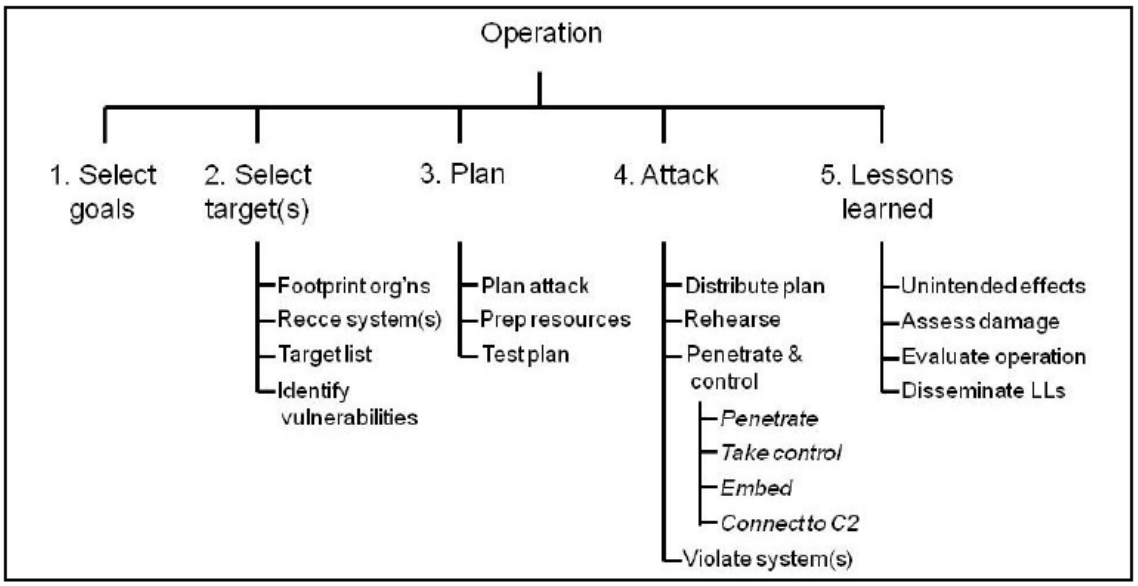

Figure 2 Canonical model of offensive cyber operations (Grant et al., 2015)

The canonical model of offensive cyber operations provides a good layout of entire cyber attack process. In the appendixes, the details of the model's processes and their subsections have been explained. In the scope of this study, the processes listed in the figure above provide enough details for analyzing high level content of each phase of a cyber conflict.

3.2 Synthesis of the chosen models

The goal of this literature review was to find models and sufficient background information for analyzing political cyber attack campaigns in detail. This means that the events must be analyzed on two overlapping planes: political or conflict plane and operational or cyber attack plane. First of these is more about the human aspect of the political cyber attack campaign, while the the other is about the technical means used.

The model phases are slightly conflicting in their way of presentation. While their essential content is not conflicted, the order of the phases is. Grant et. al. (2015) did a review of several different models which were based on both theory and empirical studies, and because of the quality of their work, the order Grant et al. used is preferred and Carr's (2011) Cyber Early Warning Model is modified accordingly to fit Grant et al.'s. (2015) Following Table 3 shows how the two models are merged.

Carr – Cyber Early Warning Model	Grant et al. – canonical model of offensive cyber operations	Note
Latent tensions	1. Select goals	The political goals are assumed to be used to choose goals of the cyber attacks.
Cyber reconnaissance	2. Select targets	Grant et al. Select targets phase content matches Carr's.
Initiating events	1. Select goals	No phase in Grant et al. model is related to this phase in Carr's model. However, this phase may affect goal selection because the nature of initiating events can be very particular and thus affecting decision making.
Cyber mobilization	3. Plan	Grant et al.'s Plan phase includes personnel-related actions, and because of this they are merged.
Cyber attack	4. Attack & 5. Lessons learned	Both models contain 'attack' phase. Lessons learned is about attacks and no other phase in Carr's model would serve as better fit, thus Lessons learned is included in here

Table 3 Synthesis of Carr's and Grant et al. models

The order of Carr's (2011) Cyber Early Warning Model's phases are rearranged as conform to the order canonical model of offensive cyber operations by Grant et al. (2015) The following figure demonstrates this change and summarizes the synthesis of the two models.

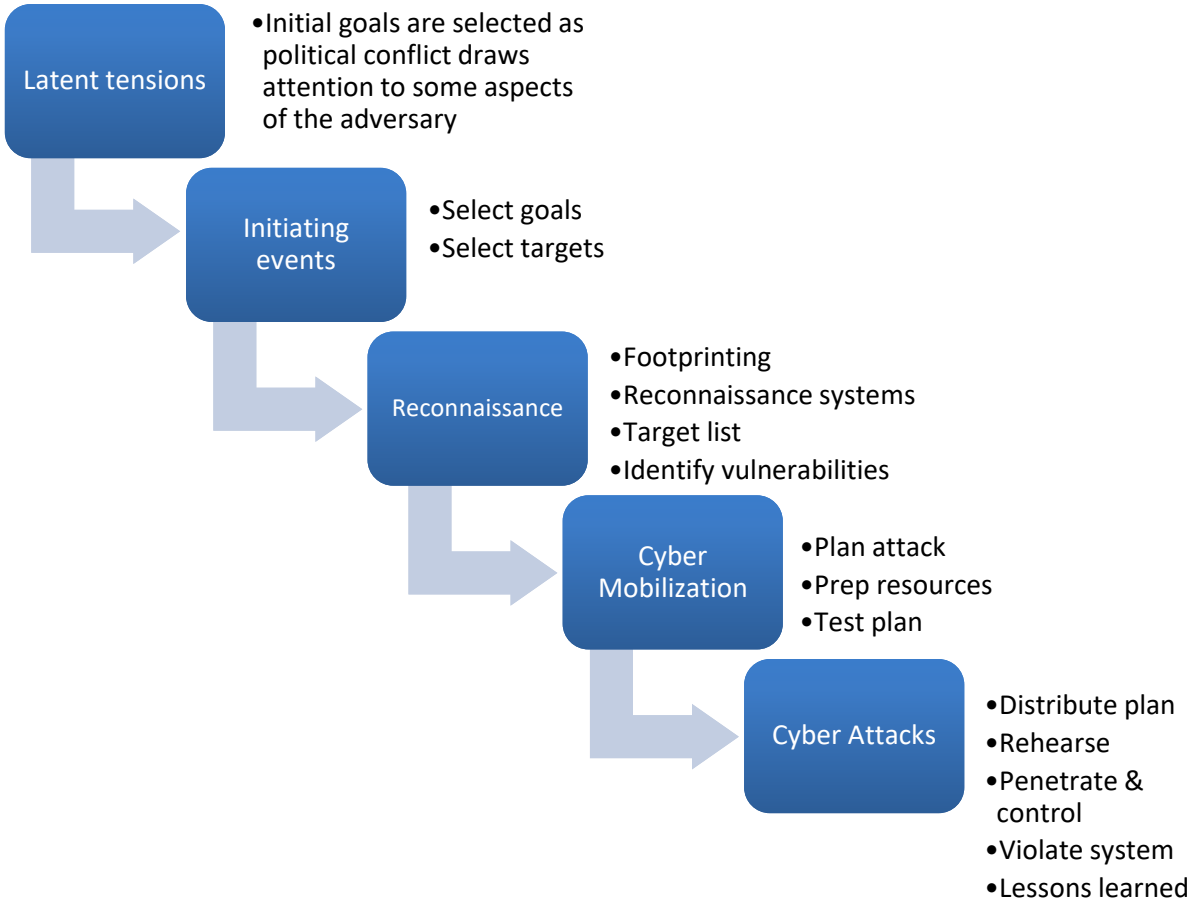

Figure 3 Synthesis of Carr's and Grant et al. models, Political Cyber Attack Campaign Model

For analysis use, on the political plane of the conflict Carr's (2011) categorization of phases is followed. Similarly, on the operational plane of the conflict Grant et al.'s (2015)

categorization of methods and their details will be used. This synthesized model is referred to as ‘Political Cyber Attack Campaign Model’.

4 METHODOLOGY

4.1 Introduction

This study is a case study aiming to construct a general picture of Anonymous hacktivists operations against ISIS. The goal is to provide a clear picture of the activities and methods Anonymous hacktivists used during the period of November 18th 2015 to 3rd January 2016.

Anonymous is not an easy object of scientific observation. The main reason for this lies in its whole essence: Anonymous is nobody and anyone can claim to be part of it at any given moment. By its loose organizational structure there is no way to claim some action, or for example a website, is really by Anonymous or not. Even though there is a circle of insiders that exert some amount of control over the collective, their influence and actions are not easy to observe either (Dobusch et al., 2015).

ISIS is no different in practice. While ISIS itself has formal organizational structure, the reality of observation doesn't change from Anonymous. Anyone can claim affiliation just by stating to support their cause. The slight difference with ISIS is that they do have formal communications channels and primitive diplomatic relations no matter how weak. They do have official channels and thus they can state their noninvolvement of any activity being done in their name (Cronin, 2015).

However, in the fragmented reality of Internet and as the web presence of ISIS is possibly loosely controlled, it is hard to say with certainty that a site claiming to be ISIS-affiliated is or is not, which applies to Anonymous as well. Thus, in this study, any website or claim made in name of either one the organizations, is assumed to be part of it. There sure can be a factor of error but as only few websites are included it is nonexistent.

This problem can also be turned around: is there a possibility that for example a website claiming to be ISIS or Anonymous affiliated would not really be? One possible explanation would be one where another group, for example a nation-state, was using the name of Anonymous or ISIS to cast blame on them for their own purposes or would like to divert their supports to certain actions that are favorable to the nation-state. Evaluating such statements is beyond the scope of this study and thus excluded from considerations.

4.2 Methods of qualitative analysis

For the qualitative analysis, netnography was chosen as the main analysis methodology. The reason for choosing netnography is that part of the content are IRC chat logs, for which suitable analysis methods are digital ethnography and netnography. These methodologies do sound similar but are not. Two key features distinguish digital ethnography from netnography. Firstly, digital ethnography sees digital sources of material as an extension of physical world instead of seeing it as its own self-sustaining cultural reality. Secondly, digital ethnography has more emphasis on quantitative methods, though qualitative methods are predominantly used. Netnography is a research method that is naturalistic; netnography does not interfere with the research subject in any way because in netnography the researcher is just a passive and possibly even unnoticeable observer. (Kozinets, 2015) The features presented here make netnography a suitable methodology for conducting this research. Also, the supplementing material from websites is also written in a very colloquial way for which netnographic methods are also suitable.

According to Kozinets (2015), a netnography research project consist of following phases which were also followed in this research.

Phase	As observed in this study
Introspection phase	Introspection phase was timed exactly at the beginning of the Paris attacks when the Anonymous campaign began. The research questions and material acquisition plan formed iteratively while following the campaign that was forming.
Investigation phase	The research questions' key content was clear from the beginning, even though their exact form was iterated several times.
Informational phase	In this phase ethical viewpoints were explored and they are addressed later in this chapter.
Interview phase	No interviews were done in this study.
Inspection phase	IRC chats and Anonymous affiliated sites were scoured through to identify candidates for this research. A far broader set of material was gathered than what was eventually used, as after few weeks into the campaign it was already clear which exact sources produced the most suitable material for scientific study.
Interaction phase	The interaction done was negligible and did not affect the results of this research. Interaction was actively avoided and goal was to be a passive observer.
Immersion phase	The IRC chats and websites were followed daily while gathering the material.
Indexing phase	This research accumulated huge amounts of data, which were indexed already by the time when they were gathered. Material was indexed by source and time of acquisition. They were reindexed when analyzing the data to relate to particular items of interest.
Interpretation phase	The material was analyzed several times over to get a clear larger picture of the chain of events and regarding the mentality of the Anonymous hacktivists.
Iteration phase	The analysis results were revised several times during this phase in an iterative manner. The overlap of the material across different parts of the used model made it impossible to do a thorough analysis without operating iteratively.
Instantiation phase	-
Integration phase	Results and recommended further research topics were formed in the end.

Table 4 Phases of netnographic study according to Kozinets (2015)

According to Kozinets (2015), there are four types of netnography, which are auto-netnography, symbolic netnography, digital netnography and humanist netnography. Of these, this research uses symbolic netnography. In symbolic netnography the goal is to focus on some specific group or phenomenon and try to understand its nature.

One key question in netnography is should researcher stay under cover or not. In this case, the purpose of joining the online IRC community was not disclosed for the following reasons:

1) All content is public. Anonymous' IRC channels are open for anyone and no registration or similar is needed; the IRC channels should be considered as open Internet forums. A webchat version of the chats was also accessible even without an IRC client by just choosing a username.
2) The material is not analyzed for communication of any particular persons or persons, but only for the content of their communication.
3) Everyone is communicating under an alias of their choice. Even though some may use aliases that are easily connected to their real-world identity, the material is not published in its entirety in this publication.

The analysis of the research data was structured around the Cyber Early Warning Model by Carr (2011) and the canonical model of offensive cyber operations by Grant et al. (2015), which were combined to work as one single model. The model was used as a basis to reflect the different phases of the conflict. The details of the Grant et al. model were not used, only the process level items were sought after in the material as the goal of this study was not to produce a detailed analysis, but a high-level analysis of how the conflict evolved. An elaboration of each of phases was produced and the information was supplemented by other sources in addition to the actual gathered research material (IRC logs and Anonymous materials). Sigholm's (2013) classification was used also for categorization of actors.

Regarding technical content and tools included in the material, the analysis was based on description given by tool authors either in readme texts or as comment lines in the beginning of the program code. These descriptions were taken as is without evaluating them further, which would be beyond the scope of this research.

While going through material pieces of data that reflected some part of the model used were indexed separately. All different documents and pieces of data were analyzed against the entire model to discern if it relates to more than one part of the model, and then indexed as relating to each part of the model as necessary.

Regarding the categorization of different information security tools referred to in research material and this chapter, tool categorization by Offensive Security (2017) was used. Kali Linux is a well-known security testing oriented Linux distribution (Orin,

2014), which was chosen because it was mentioned repeatedly in the material, apparently being a favorite Linux distribution of many for this kind of activity. The tool listing and categorization only includes tools included in the Kali Linux distribution. No conflict was noticed with the categorization by Offensive Security and with context of tools provided (if any) in the research material. Tool names and uses are provided only for additional context, as the purpose this study is not to analyze used tools in detail.

4.3 Material gathering and sampling

4.3.1 Material gathering methods

The material acquired for this study was extensive. It spans the entire public communications of Anonymous concerning the operation against ISIS from a 3-month period. After all the research material was collected it was clear that there has to be a stricter focus of the timespan of the study since the amount of IRC-log data gathered totaled some 15 000 pages in pdf converted format. In addition to that, the acquired websites that were used to share operational information totaled some 250 documents that could be converted to more than 1 000 pages.

The material for this study was chosen to be acquired from the IRC server of Anonymous. IRC, Internet Relay Chat Protocol is an application layer protocol that facilitates text-based communication between parties. IRC works with client/server architecture and is operated with a client that user installs on his/her computer (IETF, 1993).

The material was collected on weekly basis, downloading all websites linked in the topic messages. The rationale for using the topic messages is that the IRC server is controlled by Anonops.com domain which is a major Anonymous information website. Anonymous insiders are controlling the main channels and are actively banning hostile communicators, e.g. ISIS propaganda messaging users, from the IRC channels. Thus, and for the reasons stated in the previous chapter, it can be assumed to be the official message of Anonymous. Another evidence for this is the fact, that no propaganda or other hostile website was found from the links at any time which proves that Anonymous insiders did control the topic messages of channels.

The topic messages of the channels contain a short message set by channel admins, usually about the content of the channel. In this case, they also contained links to websites that had information about certain part of the operation. The content of these linked websites was collected each Monday and archived in a systematical fashion. An example is presented below.

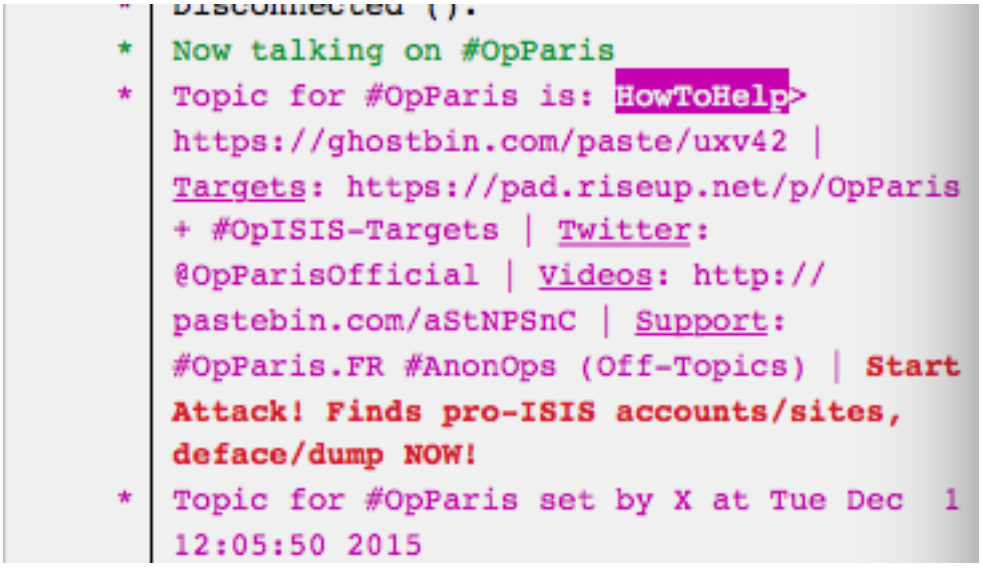

Figure 4 Example of Anonymous IRC topic messages

The information gathering was not restricted to IRC. All the links to sites in topic threads were followed and the websites were saved as copies. These were checked to be Anonymous OpParis related. Technical materials about intelligence gathering or attacks were collected to a limited extent, but the GitHub repository was examined and gathered once it was included in the topic messages as a marked source of information concerning the operation.

The channels were chosen by both browsing irc.anonops.com server channels which are freely accessible and confirmed from either other channels topic messages or from the ”Combat Index” ghostbin.com page to include all relevant channels but nothing else. Some of the promoted channels were excluded like #OpCyberPrivacy and #OpCloudflare and #OpFreeAnons that were not obviously focused on the topic of war against ISIS and would have included irrelevant and probably even misleading material in the data.

Two computers were used gather the material. The main gathering method was to store the websites samples and similar related material on a personal computer, and regarding IRC logs, also on a virtual private server that was logged in on the Anonymous (anonops.com) IRC server. This setup assured the best possible coverage of intended scope of research data.

4.3.2 Sampling

For this study, the period of starting the hacktivism campaign can provide more insight than the later phase when campaign activity toned down, and hence the period between 18.11.2015 – 03.01.2016 was chosen as the data for closer inspection. As some of the channels contained huge amount of non-relevant communication, an active and focused

channel #OpIceISIS was chosen for analysis, supplemented by #OpParis-dev and #OpBashDaesh. From the same time period, the information provided in the topic messages were also chosen for analysis as they as a whole made the spectrum of operational information provided to Anonymous members.

The comments that Anonymous members made on the channel #OpIceISIS were read thoroughly and reflected against the framework that the literature review provided. The material was analyzed several times through, both the IRC-chats and the material Anonymous produced. The website material was classified one by one to one or more columns, one column for every stage of the model. For the sake of clarity, one specific piece of material can be an object for analysis for more than one stage. Of the GitHub code repository of the operation, a version of December 21th was used, as it is in the mid-point of the observation period.

5 STUDY FINDINGS

5.1 Introduction

In this chapter, the findings from analyzing the data are presented. The chapter is divided to same phases introduced in chapter 4 “Synthesis of the Chosen Models”. In addition, and before going into the phases, an introduction of the conflict parties is presented briefly as understanding actor group backgrounds is important for putting all facts and findings into a context. In chapter 7 conclusions and limitations of this study are discussed.

Regarding terminology, earlier in this thesis it was stated that intelligence is information, something that’s made to have a context and not just raw data. In this study all data or information acquired by Anonymous is stated to be ”intelligence”, if not specifically otherwise noted. If the information is used for any kind of planning purposes it is defined as information and thus in this context, intelligence. Word “attack” is used for all kinds of cyber attacks and it will be specified as a certain type of cyber attack if necessary.

5.2 On actors and their status

5.2.1 Anonymous

Anonymous is a hacker collective. It has its roots in 4chan.org website and especially its famous bulletin board that contains random interesting and funny images from around the Internet. On the 4chan website if you post without a username, your username will be ”Anonymous”, and from that came the name of the hacker collective. The hacking began from that website’s regular’s conversations and liberal political views on current topics. The bulletin board has nothing to do with hacking, but that’s where Anonymous’ began as a hacktivist group (Shakarian P. et al, 2013).

4chan was also the place from where offensive deeds began taking place, the so-called 4chan raids. In the 4chan raids, the Anonymous members raided a certain website by some means after it had been pointed as a target on the b-board. After the 4chan the pranking culture began to move towards activism more clearly. First larger, mainstream media attention catching operation was against Church of Scientology. The method of attack was DDoS using Low Orbit Ion Cannon (LOIC), a network stress testing application that flooded the target with TCP or UDP packets. This was combined with demonstrations around facilities of the Church of Scientology around the world with the demonstrators wearing the emblematic Guy Fawkes mask. Operation Payback followed in 2010,

an offensive against American companies making copyright infringement lawsuits like Recording Industry Association of America (RIAA) (Olson, 2012).

After the first operations Anonymous retained its informal and distributed nature, but began to have some basic infrastructure and agreed conventions on doing operations, or ”ops” as they quickly came in their speak. The movement grew after Anonymous got huge media attention after the Visa and MasterCard DDoS attacks, which eventually led to some of the participants getting arrested and prosecuted. The operation began when Visa and MasterCard stopped processing donations to WikiLeaks, which at the time was the icon for privacy-oriented liberals that Anonymous attracted (Olson, 2012).

Even though being “anonymous” is at the heart of the identity, the Internet habit of using a handle, or nickname, like “0v3rl0rd” is the way of identifying individuals. Anonymity of individuals is paramount in Anonymous and members take care of preserving their privacy and secrecy of their real identities. The culture is tied a lot around Internet memes and similar Internet culture. The fact that they only exist on the Internet makes the culture and language very unique in a sense, which something that can also be seen in the material of this study.

Figure 5 A contemporary Guy Fawkes mask (Wikipedia, 2012)

The logo of Anonymous is a Guy Fawkes mask, as seen in the 2005 movie V for Vendetta, in which the mask was a symbol for avenging the oppression. Another logo is the headless suit, presented below.

Figure 6 Slate article "Recognizably Anonymous" (Slate, 2011)

According to Shakarian et al. (2013) the leadership behind Anonymous are a dozen very skilled hackers that are former members of the German Chaos Computer Club. They plan and announce the operations and handle the more sophisticated attacks. The domain anonops.com is likely to be under their control also, as well as the IRC-channels are under the domain where the anonops.com information website is hosted. Despite the openness of the Internet culture and Anonymous, there are groups and secrets within Anonymous as well. There are regional subgroups like for example Anonymous Finland, which is active according to security researcher Mikko Hyppönen (Iltalehti, 2011). Not all of these groups, like Anonymous Finland, could be found from the public IRC channels that were used in this research.

The people participating in this Anonymous campaign were likely from France and other Mid- and Southern European countries. Campaign having its base in terrorist attacks in France, this could be expected. This conclusion was drawn from the following observations:

- There were separate French and Italian translations for many of the core materials inciting people to join the campaign
- There was separate French OpParis channel
- Some participants revealed proactively being from France or Belgium, as they used French or Italian in the English channel.
- Channels had significantly less conversation between UTC 02:00 AM – 03:00 PM than outside of those hours.

From the research data, it can be seen that there was a significant number of newcomers in this campaign who did not have previous hacking experience. The anonops.com website and also the ISIS-specific operational guidance pointed out to hacking tutorials for beginners. Questions like "how do I hack" were not so uncommon the discussion,

almost daily seen in the #OpParis and also in #OpIceISIS channel though to a lesser extent.

"Nov 18 23:39:29 <mslazir> i want to help and learn more about hacking/ddosing. My programming skills are somewhat intermediate on java , C, C++ and html but that's pretty much it. Is Kali Linux a good next step?"

"Nov 18 23:36:28 <pro_anonymous> as well as dos i wanna learn how to hack email accounts web sites and defacing websites also"

These very open-ended beginner questions were left unanswered usually and at best given a link to the "Combat Index" ghostbin.com paste that had all the guides in an index. Thus, a significant part of the members participating in the IRC may not have had much contribution to the operation.

GhostSec

GhostSec is an offspring of Anonymous, an Internet vigilante group. GhostSec.org states their purpose followingly (reformatted for smaller space):

"Our mission is to eliminate the online presence of Islamic extremist groups such as Islamic State (IS), Al-Qaeda, Al-Nusra, Boko Haram and Al-Shabaab in an effort to stymie their recruitment and limit their ability to organize international terrorist efforts. This site provides a means for people to report known Islamic extremist content including websites, blogs, videos and social media accounts. Once verified by our Intel team, our operations teams set to work on removing the content. Removing content involves both official channels, reporting the content to the site hosts and requesting it be removed, and the employment of digital weapons to forcibly remove content where official channels fail."

GhostSec also states to participate in operations against child pornography, animal pornography and "CDN-misuse". GhostSec has been attacking ISIS already from January 2015, by claiming publicized attacks as their doing on their website (GhostSec, 2016). GhostSec's role in the operation has likely been crucial, as they have been involved longer in it and working with a smaller team of experts. More than a couple of times, people were referred to pass important information on to GhostSec to act on rather than do something themselves.

Figure 7 GhostSec.org front page (GhostSec, 2016)

A member of GhostSec, Mikro, was interviewed by the Atlantic (2015). Mikro claimed that they had thwarted a terrorist attack on July 2015 which was confirmed by third parties. Mikro had also moved on from GhostSec to found CtrlSec, another group with roots in Anonymous, that fights against ISIS online. In this article, a claim of taking down 130 ISIS websites was presented but not confirmed by any third party. As depicted above, at 34 days after starting their campaign they claimed to had reported thousands of websites and social media accounts.

Ghost Security Group

GhostSec is very easy to confuse with Ghost Security Group but definitely should not be. To add to the confusion, the groups have same origin but have separated paths earlier. Ghost Security Group is an organization that cooperates with public sectors in their combat against extremism on the Internet. According to their website, *"Ghost Security Group is a counterterrorism organization that combats extremism on the digital front lines of today using the internet as a weapon. Our cyber operations consist of collecting actionable threat data, advanced analytics, offensive strategies, surveillance and providing situational awareness through relentless cyber terrain vigilance."* (Ghost Security Group, 2016)

Ghost Security Group employs a dozen people in various roles and openly advertises capabilities in counterterrorism, hacking and especially open source intelligence. Ghost Security Group has, according to their blog, been involved in anti-ISIS activities also but isn't affiliated to Anonymous, unlike GhostSec (Ghost Security Group, 2016). Ghost Security Group claims to spy on ISIS and that they have thwarted terrorist attacks, but no independent sources could verify this information (BBC, 2015).

5.2.2 ISIS

ISIS, or Islamic State of Iraq and Syria, and also known as ISIL, Islamic State of Iraq and the Levant, is a jihadist Sunni fundamentalist group. The group refers to themselves rather as "Islamic State" and claims authority over all Muslims around the world as a global caliphate (Al Akbar, 2014). The caliphate has widely been rejected by Muslim groups (Akyol, 2015).

The origins of ISIS are in Jamaat al-Tawhid wa-l-Jihad (JTWJ) that was founded in 1999 by Abu Musab al-Zarqawi. In 2004 the group merged with Usama bin Laden's al-Qaida in Iraq (AQI). Zarqawi had largely more fundamentalist beliefs than bin Laden, e.g. justified killing Muslims if they are accused of heresy, and they ended up in a quarrel when Zarqawi effectively forced himself as the leader of AQI after American invasion in October 2004. Other al-Qaida leaders opposed the extreme violence that was towards Muslims as well, but Zarqawi not only continued but also merged other jihadist groups into AQI, that changed its name to Islamic State in Iraq (ISI) after the death of Zarqawi. Zarqawi was followed by Abu Omar al-Baghdadi who led ISI to gain established control of Anbar region. Al-Qaida later in 2014 disaffiliated itself with ISIS (Zelin, 2014).

In 2013 Baghdadi announced that the new name is Islamic State in Iraq and Syria, which led to conflict with the formerly merged internal groups, Jabhat al-Nusra (JN) and al-Qaida. JN was the official branch of al-Qaida in Syria and they were not consulted before the announcement and thus a struggle emerged between ISIS and JN, and they separated. The struggle has afterwards led to open war between the groups and as part of that both sides organized aggressive propaganda campaigns over the Internet, especially on Twitter. JN also did a video series of ISIS defectors. In the official rhetoric, the groups are fighting over which is the true heir of bin Laden's al-Qaida, even though the real issue are the differing opinions on Islam and jihad. During 2014, ISIS had gained a lot of territory in Iraq and Syria area, supported by steady stream of new fighters coming from abroad. They had also gained strategic logistical routes and natural resources like oil fields (Zelin, 2014).

Specialists have stated ISIS to be expert in using social media. ISIS uses Facebook, Twitter and Youtube extensively, giving a constant stream of propaganda media to its

followers and potential recruits. ISIS's use of social media is likely to be a key factor why they have managed to recruit an estimated 2000 fighters from Europe to join its cause (Khalaf & Jones, 2014). ISIS routinely and widely publicizes videos and photos of beheadings, shootings, and burning and drowning people, which guarantees media attention. The escalation of violence in their media is stated to aim at exhausting its enemies, mainly USA, mentally to yield. In addition to the brutalities, ISIS shows an image "an emotionally attractive place where people 'belong', where everyone is a 'brother' or 'sister'. A kind of slang, melding adaptations or shortenings of Islamic terms with street language, is evolving among the English-language fraternity on social media platforms in an attempt to create a 'jihadi cool'" (Ruthwen, 2015). ISIS uses war and utopia as its main thematic tools in its propaganda on the Internet, employing a wide array of social media channels: Twitter, Tumblr, Facebook, Kik, Surespot, Telegram etc. to broadcast its content. ISIS doesn't use official accounts due to the problem of them being down fast by the social media companies, but instead operate a huge number of accounts that refer to some other name (Winter, 2015)

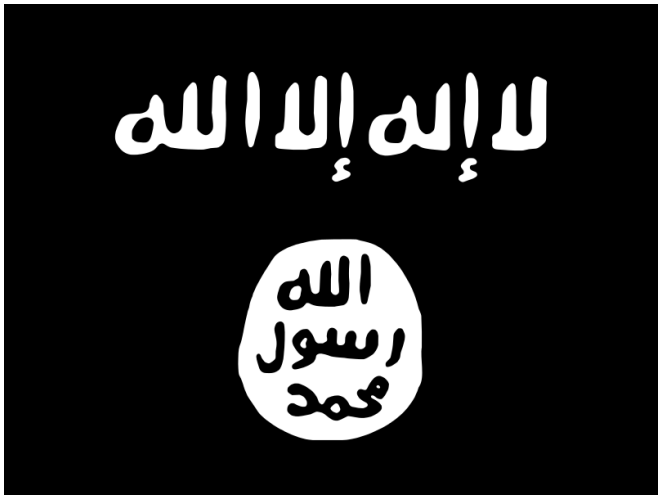

Figure 8 Flag of the Islamic State (IS) (Wikipedia, 2013)

During the campaign by Anonymous some retaliation was noticed. During the first two weeks IRC servers were down for extended periods, which was due to DDoS which was presumed to be by ISIS, though this was not confirmed. Also, during the campaign ISIS supported tried to flood the IRC chat several times in the following fashion.

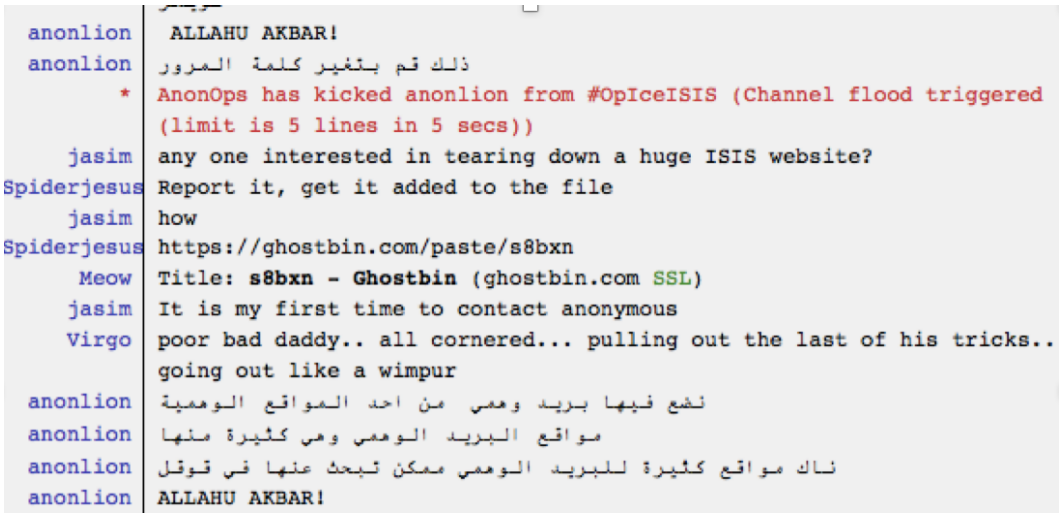

Figure 9 Example of ISIS content in Anonymous IRC chats

In the example above, user ‘anonlion’ is trying to prevent Anonymous from conducting internal communications by flooding the channel with jihadist propaganda. As seen in Figure 9, the first attempt to flood channel with jihadist content resulted already in user ‘anionlion’ getting kicked out, after which the user rejoined to continue, which resulted in a permanent ban.

5.2.3 A summary of the key facts regarding Anonymous and ISIS

While the previous sections acted as a more informal introduction to the actors that are analyzed in the study, this chapter will summarize the key characteristics of the two actors. Anonymous and ISIS will both be summarized by key facts.

The key facts are presented in the following table.

	Anonymous	ISIS
Type of actor, according to Sigholm (2013)	Hacktivist	Cyber terrorist (also: cyber militia, patriot hacker)
Founded	2004 (Olson, 2012)	1999 (Zelin, 2014)
Number of personnel	Unknown and relatively large rapid changes. In ISIS related operation, approximately 50 or so users were present for most of the time of the study in the related IRC channels.	Up to 40 000, according to latest public estimate given by US Air Forces (Peterson, 2015). It is unclear whether this includes cyber personnel and paramilitary personnel in Europe.
Legal status of personnel in conflict	- Geneva Convention laws not applicable under most circumstances - Criminal laws of country of residence	- Geneva Convention laws likely to apply to military personnel in Near East warzones - Criminal laws of country of residence
Operating area	Global	Near East, Europe

Table 5 Summary of key facts

While most of the content in Table 2 is self-evident there are couple of challenging questions. What is the type of actor of ISIS cyber operatives? As stated before, ISIS is not a nation-state recognized by the UN, but defined as a terrorist organization. Thus, defining their cyber personnel as cyber terrorists is appealing, but not necessarily accurate. Their cyber operations are defensive and psychological operations, but there is no evidence of offensive network operations outside of the DoS attacks on Anonymous servers, which were attributed to ISIS by Anonymous without providing evidence – as far as observed in the research material. Cyber militia is almost as accurate and patriot hacker is a definition they might use of himself or herself. Despite the fact that the definition can be challenged, cyber terrorist is the definition used by this study.

When do Geneva Convention laws apply to the individuals engaging in offensive cyber operations, from both sides? Short answer could be that only in the warzones of Near East if the attack is in reality encouraged by a nation-state. In reality, it is probably unlikely to have the Geneva Convention protection as cyber personnel are not necessarily officially or by their outfit recognizable as soldiers.

In most cases, and certainly with Anonymous hacktivists, they are subject to criminal laws of the country of residence. Also, Anonymous hackers may subject to criminal laws of the countries of their targets. ISIS propaganda sites were hosted globally in various

places, which weren't necessarily in ISIS territory and cyber attacks against these hosting providers' infrastructure may, and likely is, subject to criminal prosecution. Research data does not have any indications of such activity happening. On a related note, Anonymous' guides instructed members to use Tor network, virtual private servers and VPNs servers to hide their true location, which may have prevented any criminal prosecution from happening.

5.3 Latent tensions

As defined by Carr (2011), latent tensions are any and all tensions, grudges or animosity between two political groups. Analyzing the actual clear tensions is difficult regarding Anonymous. One way would be to analyze the research data, but the data is after the Paris attacks and thus characterized by the attack, which is why it would be incorrect to use post-attack data to explain pre-attack tensions. In the scope of research there are no discussions included in the material prior to Paris attacks. It is also very likely that these discussions were very randomly placed both time-wise and between different then existing IRC-channels, and the decision to launch Operation Paris might have been done by the insiders which would mean that there is no public data available on the discussions.

All this being said, the tensions can still be deduced, as the core values of both groups are fundamentally very different. The values that ISIS presents are conservative and restrictive, from the very religious worldview. They also promote violence, control and oppression, and despise science. (Alkaff, 2015) Anonymous is almost the exact opposite.

According to Huang (2015) " - - many Anons [Anonymous members] do not have a clear political agenda, their actions made Anonymous moniker take on a political coloration. This is because Anons' motive is not about monetary theft or pure security exploitation. In the past five years, people who paid attention to the work of Anonymous have noticed this collective more frequently engaging itself in the self-claimed mission of defending freedom of speech, hacking "wrongdoers" and revealing imperfections of the social mechanism". By reflecting on their targets, with the likes of Church of Scientology, Visa, MasterCard, Sony, Saudi government, Canadian government, Parliament of Uganda, one could claim that motivations are mainly for promoting liberal policies, as all the attacks have been preceded by some restrictive, anti-homosexual, anti-piracy, anti-privacy or related action by the targeted party. Anonymous also has several times stood up against violent practices, first in Operation Darknet against child pornography and then in Operation Hunt Hunter against a revenge porn site, and in 2012 against Israeli websites in Operation Pillar of Defense, retaliating for Israeli violence in Gaza area.

In the discussions included in the research material, there was general fear regarding new possible attacks by ISIS. Related to this possibly, were the often occurring hateful mentions about ISIS. In two examples above nicknames pro_anonymous and nemesis999 are expressing their feelings in the IRC chat:

"Nov 18 22:27:59 <pro_anonymous> together we can fight this disease"

"Nov 24 15:08:43 <nemesis999> isis must be wiped from the earth or there will never be world peace."

The disgust towards ISIS and terrorism was also demonstrated in nicknames used in the IRC chats:

*"Nov 24 04:20:27 * DaeshDespizer is now known as nemesis999"*

"Nov 24 22:32:58 <Terrorist-Tracker> hi to all bro"

Fear for their own safety, expressed in a variety of forms, is also seen as a theme in the research data:

"Nov 18 18:08:40 <boofhead> I know im a newbie here but i support all the work all you guys are doing worldwide should be proud of yourself in providing security to your countries abroad thank-you all and your all doing more than the LEA , great to have guys likeyourself worldwide"

"Nov 18 18:33:03 <Infinitus> Any news on the threat level present in the UK"

"Nov 23 10:06:31 <Tango> Isis are hating France real bad"

The research data does not reliably reveal the actual values conflict that resulted in Anonymous collective members being interested in attacking ISIS. However, it is clear that one motivating factor was fear for their own safety, partly turned as hate towards ISIS, have together likely pushed many over the threshold to take action. As elaborated previously, the values conflict was likely under the following themes: freedom of speech, freedom of religion and violence as a method for promoting policy.

5.4 Initiating events

5.4.1 Paris attacks

Initiating events are the events that push one or more parties with latent tensions to make an action (Carr, 2011). In this chapter, a brief description of the November 2015 Paris attacks is given.

On Friday evening of 13 November 2015 seven coordinated terror attacks were carried out in Paris killing 130 people. The attacks launched almost simultaneously. First ones to take place were two explosions close to Stade de France, followed by gunmen opening fire at the site of Petit Cambobge, Rue Bichat and Le Carillon restaurants. The same gunmen continued then to Casa Nostra pizzeria, to La Belle Equipe Bar and finally to the Bataclan Theatre in which caused most casualties, 89 losing lives. During the evening a third bomb was detonated, also near Stade de France. The attackers were driven to upper floors of the Bataclan by anti-terror swat team, and all but one of them were either shot or blew themselves up with the suicide vest. Two of them were later killed during Saint-Denis police raid. The terrorists plotted another attack at La Défense at a shopping center and at the Charles de Gaulle airport, but the attacks were never carried out. Several bomb threats were made for flights during the aftermath but no bombs were found from the planes (Telegraph, 2015).

The attackers were of French, Belgian and Syrian origin working as a group, but all were EU nationals and had no difficulty moving around Europe (Traynor, 2015). Some of the members of the group had previous arrest warrants related to terrorism and trips to Syria. They knew each other through very varying connections, either met in Syria, Brussels and some even in jail. Two of them were brothers. It remains unclear how many attackers there were in total as the search still goes on. Turkey had notified France about the suspects a year earlier and as mentioned previously, some of the perpetrators were already on the terrorist watchlist as potentially violent extremists (Telegraph, 2015).

France raised the highest level of national security alert after the attacks and president of France, Francois Hollande, gave a historic speech at Versailles to the upper and lower houses of parliament, something that has happened only two times before during the last 150 years. During the weekend security forces, arresting people and seizing weapons, conducted several anti-terrorism raids. France also carried out intensive strikes in the town of Raqqa, the unofficial capital of ISIS. France activated Article 42 of EU that calls for other member states to assist with military means the calling distressed member state (Telegraph, 2015).

5.4.2 Anonymous' reaction to the attacks

The aggression was initiated from the side of Anonymous and ISIS has no publicly claimed quarrel with Anonymous, as far as was observed in this study. On 16 November 2015 Anonymous declared war on ISIS in a Youtube video (Anonymous Italy, 2015). In the video, an Anonymous Italy spokesperson expressed worry about events that have taken place and encouraged people to join their cause to hack and expose ISIS online in new Operation Paris. Anonymous very quickly announced taking down couple of thousand accounts (number seems to differ a bit depending on source) on Twitter (Baker, 2015).

Below is the speech given in the Youtube video, as provided in text by Anonymous Italy (reformatted, content unchanged):

"Hello citizens of the world. We are anonymous.

The aftermath of Friday, November 13, 2015. France is shocked by the events caused by terrorism in the capital. We first wish to express our sorrow and our solidarity with the victims, the injured, and their families. To defend our values and our freedom, we're tracking down members of the terrorist group responsible these attacks, we will not give up, we will not forgive, and we'll do all that is necessary to end their actions.

During the attacks of Charlie Hebdo, we had already expressed our determination to neutralize anyone who would attack our freedom. We'll be doing the same now, because of the recents [sic] attacks. We therefore ask you to gather and to defend these ideals. Expect a total mobilization on our part. This violence should not weaken us. It has to give us the strength to come together and fight tirrany [sic] and obscurantism together.

We are anonymous.
We are legion.
We do not forgive.
We do not forget.
Expect us."

This declaration was also published in French and Italian. The texts were included in the research material. Some Anonymous members had very strong feeling about the importance of their work and strongly felt a need to help:

"Nov 18 18:08:40 <boofhead> I know im a newbie here but i support all the work all you guys are doing worldwide should be proud of yourself in providing security to your countries

abroad thank-you all and your all doing more than the LEA , great to have guys likeyourself worldwide"

"Nov 18 18:09:33 <anonish> thanks man bu we are doing what is right. its what i would expect from anyone capable"

"Nov 18 18:50:43 <RudeBoyBE> trying to find out how to help Anonymous against Daesh"

One could see certain similarity with huge number of Americans enlisting to military after 9/11 terrorist attacks (Winokoor, 2011) – citizens wanting to eagerly find their way to help and strike at the perceived enemy. The enemy mentality was clearly noticeable in the research material, as noted in examples earlier also. Hacktivism was obviously not seen as a way in 2001; the Internet was still very much developing and world was recovering from dotcom crisis at that time. Time will show if hacktivism will continue to be seen by the public as an alluring way to strike at the enemy instead of conventional military ways.

5.4.3 Anonymous' goals and target selection

From the research data, the high-level goals and subsequent target selection can be observed. It must be noted that 'goals' is quite vague definition here as with Anonymous everyone picks goals they see suitable.

Two key themes were noticed. All facts related to tools and tactics presented below will be explored in following chapters.

- Denial of Service on ISIS affiliated websites.
    - Denial of Service attacks were the most discussed form of attack in the IRC conversations, which will be described later in 6.7.4. section.
    - There was a dedicated DDoS chat for the campaign, #opddosisis. The channel had so called 'no lurker' policy, which means passive participants did get banned from the channel fast. This may be due to the fact that some participants were possibly using illegal botnets (in contrast to voluntary botnets used also in the campaign) and they did not want security researchers and law enforcement get knowledge about the botnets via this IRC channel. This is also the reason why not much of the conversations was captured in the research material.
    - Github repository contained several different DoS and DDoS tools. Included were e.g. several versions of SlowLoris DoS tool (Appendix 4).
- ISIS propaganda and recruitment communication suppression in social media.

- Most of the tools distributed via IRC topic links were related to either social media account reconnaissance or social media account takedown, (Appendixes 4 and 5, discussed in detail later).
- The Github repository contained 18 different social media reconnaissance and account takedown tools (see Appendix 4).
- Social media accounts were actively searched for and linked to in IRC chats, see examples later in 6.5.1.
- Anonymous had a distributed voluntary botnet for social media reconnaissance and reporting procedures. The botnet tool was called TwitPort. Instructions for participation were distributed during some of the weeks included in the research material, as can be observed from Appendix 5 Table 15 – mobilization ("botnet participation instructions").
- Another attack vector used was "hashtag spamming" for which a tool was developed. The goal was to make it impossible to follow the targeted ISIS affiliated hashtag as the spam content would fill in most of content posted with the given hashtag.

Other goals were also discussed. Doing "psyops" and injecting "countermessaging" to ISIS conversations was a growing sub-operation in the latter half of the research period. Psyops is shortened version of term psychological operations, that can be defined as distributing selected meanings, emotions and messages to a certain audience to achieve influence on their emotions and thinking (Rouse, 2012). Countermessaging was defined by Youth Department of the Council of Europe (2017) being "- - *a form of counter narrative, which can be used to directly de-construct, discredit and demystify violent extremist messages*". #OpBashDaesh was the name of this operation, which was very different from other operations being non-technical. An excerpt from the website, opbashdaesh.com, dedicated to the campaign outlines the motivation and goal behind #OpBashDaesh:

"The time has come to directly attack Daesh's supply of foreign volunteers. Daesh manipulates vulnerable teens and young adults by creating a propaganda bubble, a distorted reality promising an impossible utopia.

This Op aims to puncture that bubble, to force Daesh recruiters to face hard questions about Daesh's mistreatment of foreign recruits, brutality towards sunnis, and the existence of groups like the YPG that strike terror into Daesh's hearts while saving innocent Muslims.

This is the most socially mediated war in history. You can help deprive Daesh of foreign recruits. If not by spreading the truth online, then spreading it among your community."

‘Hacking’ ISIS websites and other servers was also discussed. The goal of this broadly stated ‘hacking’ was rarely mentioned, though few times it seemed to be Denial of Service by using administrative privileges to shut the site down – sometimes the opposite.

“Nov 20 21:49:44 <Sidious> Stop taking down shit! Hack, Obtain, MAINTAIN!”

“Jan 06 21:12:04 <Drastic>z3us, should i hack www.tajdeed.org.uk ?”

Defacing, the act of placing new content on the site or redirecting it to other site, was also mentioned several times. Defacing may be used to broadcast a message to the people intending to visit the site, or just deny access to the content (i.e. Denial of Service).

“Nov 19 06:48:53 <Anonymous9> TheKingSupreme: Well DDOS is one option, but a better option is to first see whether they can be hacked or defaced”

“Nov 28 01:45:18 <s33m5_l3517_> soooooooooooo my fellow anons and hackers ! i´ve found an isis website (wordpress) and collected some data and possible exploits , maybe someone wants to help me with the defacement of the page ... hoewever here is the link https://ghostbin.com/paste/75zfr”

“Nov 28 01:53:44 <s33m5_l3517_> trapbant: do you really think so ? :D i think we could possibly hack into the admins acc / get the priviliges since its possible to upload an "image" with a payload to the timthumb interface”

This chapter can be concluded with a short summary. Goals were mainly related to suppressing social media communications, mainly on Twitter. Most other hacking activity seemed to have the first mentioned goal of producing Denial of Service condition in some form to the ISIS websites, preventing ISIS supporters from communicating and reading about ISIS. It should be noted that result of producing Denial of Service condition on website has exactly the same result as social media takedowns – suppressing communication channels.

5.5 Cyber reconnaissance

Cyber reconnaissance aims to acquire information that can be used find a weak spot in target system or organization, as defined earlier in 2.2.1. In military and foreign policy context word intelligence is also used. These terms are used inter-changeably in this text. First, the role of reconnaissance will be analyzed in the context of strategy, and secondly, the tools used for reconnaissance will be analyzed.

Reconnaissance and in general acquiring information about targets played a key role in the operation from the first day, as can be seen from the excerpt below. Judging from the fact that Anonymous insiders who controlled the IRC channels clearly told Anonymous members via the IRC topic messages not to attack during the first two weeks, but to first focus on gathering information, they likely saw that the fragmented web presence of ISIS needed a structured approach if any effect was to be accomplished. ISIS's attack surface consisted of thousands of social media accounts, hundreds of small recruitment or informational websites and some server & network infrastructure.

The Anonymous members controlling the IRC servers clearly had the high level strategy of first doing reconnaissance and then attacking – see following IRC topic messages (emphasis added):

*"Nov 17 12:20:35 * Topic for #OpParis is: Operation Paris Video: FR> https://youtu.be/jPDcYWiycY8 EN> https://youtu.be/g-qGl4mVTuY IT> https://youtu.be/oZPucyvPiwc | HOW TO HELP: http://opparis.cf & https://pad.riseup.net/p/OpParis_TARGETS | Twitter: @OpParisOfficial | Live: https://www.reddit.com/live/vwwnkuplwr9y | French: #OpParis.FR -* ***No DDOS/Defacing, just collect targets!*** *- Get your off-topic chat to #anonops"*

Which was later changed to:

"Dec 07 18:33:13 -Paris/#OpParis- Channel Topic: HowToHelp> https://ghostbin.com/paste/uxv42 | Targets: https://pad.riseup.net/p/OpParis + #OpISIS-Targets | Twitter: @OpParisOfficial | Videos: http://pastebin.com/aStNPSnC | Support: #OpParis.FR #AnonOps (Off-Topics) | ***Start Attack! Finds pro-ISIS accounts/sites, deface/dump NOW****!"*

Also, this strategy could be seen in guiding the non-experienced members to collect information, verify targets and then give the targets to the GhostSec group or to other repositories used. It can be assumed that these targets from reconnaissance were feeded to more experienced members who were doing the attacking. For example, from the IRC chats it cannot be said who controlled the voluntary social media botnet TwitPort, which was used during the first weeks in the campaign. In addition to that, on the IRC server there was a channel named '#opisis-targets', to which some members guided others to make their submission regarding possible targets, which would be subject to "verification". Example below from #opisis channel:

"Feb 01 10:34:46 <m3ph1st0> please submit targets to #opisis-targets for verification"

5.5.1 Footprinting and system reconnaissance

This section combines, for brevity, Grant et al. model processes footprinting and system reconnaissance. Footprinting is defined by Margaret Rouse (2007) on TechTarget blog as "*In computers, footprinting is the process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment. Footprinting can reveal system vulnerabilities and improve the ease with which they can be exploited*." This differs slightly Grant et al. model, in which footprinting is the first step and then further reconnaissance and vulnerability identification produces vulnerability information. Grant et al. definition is used here. In this section, tools and methods related only to finding topical information about systems, such as OS version, IP address and similar will discussed. This means that all reconnaissance tools are discussed except those capable of gathering detailed information enough to recognize exploitable vulnerabilities, which are discussed later in this chapter.

Most mentioned footprinting tool was Nmap, 14 times in the #OpIceIsis IRC chat. Several Nmap scan results containing system information, including for example IP address and operating system type and version, were included in Github repository and links in IRC. For example, in the research material a Ghostbin paste (2fqcg) included large amount of Nmap scan results. Nmap is a well-known and widely used open source tool to scan a target computer for information that can be used for finding vulnerable machines (BBC, 2003). A snippet of the paste and the included Nmap scan results is provided below:

"Here some details about targets from list https://ghostbin.com/paste/s8bxn
A full simple list (clean/ordered) of targets : https://ghostbin.com/paste/22djn

Cloudflare direct IP by using http://www.cloudflare-watch.com/cfs.html#box OR http://www.crimeflare.com/cfs.html#box

Ports scan by using nmap -sV -O -P0 x.x.x.x OR nmap -sV -v -T4 -O -PN x.x.x.x

--- part removed for brevity ---

http://www.albayanislamac.com/
CloudFlare NO
Direct IP : 94.75.198.107 HOLLAND

NMAP Output :
21/tcp open ftp Pure-FTPd

26/tcp open smtp Exim smtpd 4.85
80/tcp open http Apache httpd
110/tcp open pop3 Courier pop3d
143/tcp open imap Courier Imapd (released 2011)
443/tcp open ssl/http Apache httpd
465/tcp open ssl/smtp Exim smtpd 4.85
587/tcp open smtp Exim smtpd 4.85
993/tcp open ssl/imap Courier Imapd (released 2011)
995/tcp open ssl/pop3 Courier pop3d

Web application information : Update 22-11-2015 : SERVER NOT FOUND"

In the example above, the Anonymous members have used Nmap port scanner to scan various potential targets that they had identified as interesting. This particular piece also identifies other interesting curiosity: apparently ISIS system administrators used United States based CDN (Content Delivery Network) provider CloudFlare. In CloudFlare's CDN service DDoS (Distributed Denial of Service attack) protection is included, and thus if Anonymous recognizes that an ISIS site is behind CloudFlare CDN, they could not use DDoS methods to attack this particular site. This was widely discussed during the campaign - even a separate channel, #opcloudflare, was set up but the content of that channel is beyond the scope of this study.

In addition to Nmap, some other technical sources of footprinting information were likely used. No significant amount of footprinting and reconnaissance information at scale was present in the material. This does not mean it was not done at all and/or in a systematic fashion. What could be concluded from this is that Anonymous members participating and active in the public IRC channels did not do reconnaissance in a large scale or systematically. Subgroups with more experienced members operating elsewhere on closed IRC channels may have been conducting more professional and systematic reconnaissance operations.

Also, footprinting and reconnaissance in the campaign included recognizing ISIS affiliated websites and accounts on social media. While social media reconnaissance does not fit the description of footprinting provided above, this is the most suitable part of Grant et al. model for including and discussing the various social media reconnaissance tools and methods employed by Anonymous in the campaign. There were several tools written specifically for either recognizing keywords and phrases related to ISIS. The sophistication of the tools extended also to recognizing ISIS flags out of pictures. The extent

to which these tools were used, is unclear. In the GitHub repository there were 41 different reconnaissance tools which of most were related to social media reconnaissance, focusing mainly on Twitter. The tools were capable of:

- Scanning for hashtags and retrieving account names on Twitter
- Scanning for followers of accounts on Twitter
- Scanning for keywords in tweets on Twitter
- Scanning for keywords on websites
- Recognizing ISIS flags on any website
- Crawling Google results for keywords
- Downloading user data from Twitter user accounts

What could be concluded from these observations is that Anonymous members clearly searched for multiple ways of recognizing ISIS content, aiming to recognize jihadist messages across the web. Most technically sophisticated were the OpenCV neural network based image recognition bots that were scouring websites with ISIS flags.

Social media target reconnaissance was done manually also. The IRC logs contained more than 1300 messages including mentions of Twitter, Facebook or Instagram accounts. In #opiceisis and #opisis channels, respectively, following messages detail this discussion:

"Dec 15 22:22:56 <taikenhead> Yeah, gone after over 300 accounts so far, they keep coming back. I just reported this one too: https://twitter.com/77Grudjeiw"

"Dec 28 06:39:54 <taikenhead> Here is a guy on Twit who I don't report and keep links to other ISIS members fresh through.Bookmark his link and go through some of their profiles and they often list links to sites. https://twitter.com/abcd28688"

Some if these messages were plain links to ISIS accounts, like these examples on #OpParis:

"Dec 16 23:30:06 <aski> https://twitter.com/falahalsha4"

"Dec 23 14:55:28 <dungeon_master> https://twitter.com/muraqib__111"

5.5.2 Target listing

Target listing is a process that provides as output an actual target list and provides input for vulnerability identification process (Grant et al., 2015). In the material, various target

lists were included. These targets can be further divided into IP-based targets and social media-based targets, meaning that target is either based on some IP address or is an entity on a social media platform.

During all the weeks included in the research material, several target lists were being distributed. These target lists did not change significantly after the first weeks of the campaign for unknown reasons. Possibly creators of these lists became inactive or just did not update these specific lists. There was simultaneously several target lists being distributed. Also, there was a reporting site under GhostSec.org that was advertised several times in IRC, from which the targets are assumed to have been consumed by GhostSec.

The format of target lists was usually raw text data, one target per line, usually posted on some of the paste sites like Ghostbin. The format was likely this because raw text data with one target per line can be used as input for most vulnerability scanning and attack tools mentioned in the campaign. Furthermore, this the format in which quite many tools that could have been used have produced it. Example of this is below (Ghostbin paste 22djn from 15.12.2015):

"Full list of ISIS websites without http or https or www.
I also removed some duplicate entries like www.Albuxoriy.com and www.albuxoriy.com
Sorted and unique from the list https://ghostbin.com/paste/s8bxn

Details of each on : https://ghostbin.com/paste/2fqcg

4342.alamontada.com
ahlamontada.com
albayanislamac.com
albusyro.info
albuxoriy.com
alemara1.org
alfajrtaqni.net
alfidaa.biz/vb/"

--- rest removed for brevity ---

Regarding both IP-based and social media based targets, the target listing procedure and format was similar. Sometimes they were even included in the same documents, possibly just to avoid creating multiple pages. IP-based targets were reported either by their IP address or by their DNS name. The latter is arguably the more effective way as quite many of the sites were in virtual hosting or behind CloudFlare CDN, in which several

sites are behind the same IP address. Related to this, several tools created for the campaign were capable of scouring the target lists for sites behind CloudFlare and figuring out the site's real IP address.

5.5.3 Identifying vulnerabilities

Identify vulnerabilities process produces software and hardware vulnerabilities as an output in the Grant et al. (2015) model. In this section tools and methods for this are discussed.

Regarding tools used, most used tool for identifying vulnerabilities was sqlmap. This tool can be used to identify SQL-injection vulnerabilities in databases and software accessing the database. (Damele & Stampar, 2017). In addition to that, Nmap was mentioned, as Nmap can also be used for identifying vulnerabilities (Offensive Security, 2017). Other tools that were discussed were Uniscan, Vega, w3af and WPscan.

Vulnerabilities were either mentioned in IRC chats or posted on Ghostbin or Piratepad for further use. Example of this is presented below (piratepad.net/FTG6N0mVG4):

"This pad is for posting GHOSTBIN's to Vuln Scans/discovered 0day exploits/other scans that will help us deface/root/hack IS websites.

Please tag your scans with your handle!!

===== VULN SCANS ==
https://ghostbin.com/paste/f2o8d - Korrupt - CyberKov Vulns [!Use A VPN!]
https://ghostbin.com/paste/9a9oq - Korrupt - http://el-tewhid.com - Multiple Vulns Discovered. BruteForce is not a good option, it blocks proxy's and logs incorrect login IP's.
https://ghostbin.com/paste/r4y33 - Voxi - SQLi found on http://radioandalus24.com
https://ghostbin.com/paste/pqfpd - Korrupt - http://anti-majos.com - Multiple Vulns Discovered.
https://ghostbin.com/paste/43kor - Mohan_ [SQLi and full (non-invasive) report of hizb-afghanistan.com (WHOIS, TRACEROUTE, etc)]

Have fun guys :]"

In the example above, an ad-hoc group is gathering vulnerabilities they have identified in ISIS affiliated systems. It seems like the participants going with handles 'Korrupt',

'Voxi' and 'Mohan_' have been running automated vulnerability scanning tools, and they have linked the reports on this public web page for later use.

No significant amount of information regarding vulnerable systems were included in the research material, which is why not much can be reliably discerned of Anonymous' vulnerability identification process. The lack of information would make sense, because posting the information publicly would reveal it possibly to ISIS making them able to patch the systems.

5.6 Cyber mobilization

5.6.1 Methods of mobilization

In this section findings on mobilization methods are included. This was part of Carr's (2011) model as it was based on crowd-sourced scenarios also, whereas Grant et al. (2015) model assumed that model is applied to strictly controlled nation-state actor.

Anonymous communicates to its members through various social media channels to which links were included in the material. Even some subgroups inside the campaign had their own social media accounts. Throughout social media websites there are numerous accounts in the name of Anonymous, usually a modified version of words "Anonymous" or "Anonops". For a casual onlooker, it is hard to tell how authoritative each one is in reality and one can even ask how relevant it is to question how authoritative a website or social media account is as a voice of Anonymous. There are several Twitter accounts, Facebook pages and Youtube accounts are likely controlled by some Anonymous members. In this case, it was the Anonymous Italy Youtube account that acted as the first rallying party for guiding interested people to the Anonymous' IRC-chat.

Included in the IRC specifications (IETF, 1993), IRC channel may show a 'topic' message that is seen by everyone joining the channel. Anonymous distributed guidance to members via the topic messages that each channel had in the following manner:

"Dec 08 17:51:01 --- Topic for #OpIceISIS is ## || Newbloods read: https://newblood.anonops.com/ | http://pastebin.com/7y1RvA6V/ || https://vid.me/8Wds || DDOS https://ghostbin.com/paste/s8bxn ## Other channels of interest: #opddosisis #OpCyberPrivacy || Guide 1# http://pastebin.com/H8rJsq4r || TwitterReporter http://pastebin.com/tRv0jSfu || Target ---> http://pastebin.com/kidbjz3e || combat-index || https://ghostbin.com/paste/uxv42 || ##"

The example above highlights the Anonymous common method of communicating important guidance and documents to members – they are provided as short links. These

links usually point to pastebin.com, ghostbin.com, piratepad.com and some other similar websites that provided text-based simple pages for distributing raw text information. After the first weeks, an index page called Combat Index that was published and kept update in English and French, as a large number of participants were French speakers. Combat Index page was essentially itself a huge link collection that included most of links distributed around the channel topic messages. Also, some Italian material was present, but almost all of the technical guides were in English.

5.6.2 Attack planning

Two levels of attack planning in the campaign can be discussed, which are campaign-level attack planning and target-specific attack planning. Attack planning results in resource specifications and an attack plan in the Grant et al. (2015) model, which is evaluated here.

On campaign level, the concept of attack planning is fairly vague but can be observed to some extent. As noted earlier 6.5.1., the IRC chat topics contained first instructions for gathering information about targets ('reconnaissance') and then starting the attacks. Also, the targeting strategy can be somewhat reliably be discerned to be to takedown communication channels, social media accounts and support websites more specifically, as noted in 6.4.3. No resource specifications or concrete attack plans were found in the material, though the need for social media takedown capabilities was addressed in several discussions.

On the target-specific attack planning the attack planning process was very dynamic. The plans were formed in IRC chats and did not have any further documentations or specifications. Once a suitable target was noticed, members began searching for possible vulnerabilities and attacking. In other words, between the reconnaissance and attacking there was very little attack planning, which is the topic of this chapter – or at least it was never present or discussed in the open IRC channels. As far as research material shows, there was no control of this process but only rather members notifying each other what they were doing at the moment and asking for others to support the process. An example of this is below:

"Dec 30 14:38:34 <Drastic> z3us, just a question, is abuqatada.com on our targets list ? i dont wanna work it uselessly

Dec 30 14:39:12 --> Davincii (Davincii@AN-fdm.0m8.e7l8s0.IP) has joined #OpIceISIS

Dec 30 14:41:39 <-- Datamoni has quit (Quit: Web client closed)

Dec 30 14:41:45 <Z3uS> yes

Dec 30 14:41:53 <Drastic> alright
Dec 30 14:42:01 <Drastic> im working on it
Dec 30 14:42:12 <Drastic> ftp.abuqatada.com - 85.17.153.205
Dec 30 14:42:13 <Z3uS> mkay
Dec 30 14:42:23 <Drastic> ill crack their ftp as root
Dec 30 14:42:38 <Drastic> already doxed, now looking for vulns
Dec 30 14:43:04 <Z3uS> dump db if possible
Dec 30 14:43:36 <Drastic> after vulns scanner is done
Dec 30 14:43:45 <Drastic> want the dox info ?
Dec 30 14:44:37 <Drastic> ISP is in netherlands
Dec 30 14:44:43 <--fear has quit (Quit: Leaving)
Dec 30 14:44:55 <Z3uS> pm it
Dec 30 14:44:59 <Drastic> okki
Dec 30 14:46:31 --> Silverlizard (silverlizar@AN-grd.m2c.uc5ucc.IP) has joined #OpIceISIS
Dec 30 14:46:52 <Drastic> done z3us"

Similar pattern of discussion can be observed occurring multiple times in the material, though most of the time it seems to be even more uncontrolled. This may be due to several possible factors. It could be that members were rarely doing attacks so complicated that planning was needed or that Anonymous members did not have experience in cyber attack planning. Material and conclusions presented in this study support other observations that participants in the public channels were relatively inexperienced, which is why the two possible factors explaining the lack of planning are quite possible. It must be noted, that more structured attack planning may have been done in private chats or channels, by groups of more experienced members like that of GhostSec, which was discussed earlier.

5.6.3 Resource preparations

Resource preparation is a process that is difficult to notice in detail regarding specific attacks but possible to identify on campaign level from the research material. Grant et al (2015) implicitly define resource preparation as a process that results in 'deliverable weapons'. For single operations against any target no significant resource preparation was noticed.

On campaign level, three forms of resource preparation were identified:

1. Development of campaign specific tools. Examples of this are the Twitter Reporter tool and other similar social media-related tools. While it is impossible to determine with 100% reliability the origin of these tools, the fact that they

had appeared to campaign's GitHub code repository with campaign specific elements in the code, e.g. keyword lists, is indicative of campaign specific tool development.

2. Gathering existing tools, mainly related to information security, that can be used in the campaign.
3. Organizing material to Github. Github contained source code of all campaign specific tools and other generic and useful cyber reconnaissance and attack tools.

It can be concluded that resource preparation was done extensively. Firstly, the social media takedown tools that are by their nature attack tools as they damage ISIS's ability to communicate. Similarly, delivering cyber attack tools to campaign participants can also be considered to have the same nature of delivering weapons, even though these cyber attack tools are freely available in the Internet as well.

Main part of the technical material, such as scripts, was distributed either through the GitHub code repository or with a Ubuntu VirtualBox image, "FuckIsis.ova". Ubuntu is a Linux distribution and VirtualBox is a virtualization technology that allows an independent operating system be run inside the host machine, giving for example a Windows user ability to run a Linux machine on his/her Windows host computer. The image had a preloaded set of all the essential tools and scripts used in OpParis. It is hard to say how popular the image has been. The code repository was updated constantly and expanded rapidly in the first two months and achieved its some sort of maturity by the end of December, as it wasn't updated after that in any major fashion. By 3.1.2016 the repository contained hefty 800MB of scripts and other information text-format.

As a curiosity, there was also a hashtag spamming tool, twitterhashtagspammer.py, that could spew huge number of tweets for a given hashtag, making this spammed content dominate the content of the given hashtag is searched for in Twitter. In Github, there were a total of 7 social media tools which of 6 were for Twitter and one for Facebook. Some of these were also distributed via IRC topic messages.

A noteworthy thing is that the repository also contained directory named "Hacking school" that was linked to in the Combat Index and several other beginner guides as well. The Hacking School folder included very basic text guides to networking scanning, SQL injections, Internet privacy and introduction to server hacking software.

Of all the material in the Hacking school directory, the most interesting piece was a one-pager why an amateur should not participate or try to hack anything regarding ISIS. This note was also distributed via pastebin to some channels. This writing outlines the counter argument, being against all other material that plainly recommended Anonymous members to participate and 'hack' ISIS. The writer gave five different reasons not to participate, which of the first one explains writer's rationale quite well:

"Want to help fight Daesh? Make sure you're not doing more harm than good. Otherwise, you may as well be on their side.

First, realize that you are a civilian stepping into a digital battlefield that is directly linked to a physical battlefield. If you DDOS an NSA-monitored deep web Daesh chat, you may well cut off actionable intelligence about where an ambush is being set up. You could be the cyber equivalent of a civilian poking his head out in a firefight, blocking a direct shot at a high value target."

Other reasons the writer outlined were: secondly, should the reader, as a non-experienced civilian think the he/she really could be of help; thirdly, random targeting targets innocents possibly provoking islamophobia; fourth, common Anonymous method have not had much success with terrorism; and lastly, one should question one's real motives in participating in the campaign in the first place.

5.6.4 Testing the plan

No indication of testing plans was noticed in the research material. This is not surprising, considering that Anonymous does not have, according to any resources present in the research material, environments for practicing. Nor does the nature of participants encourage any kind of testing; participants often mentioned using VPNs to hide their origin thus making any consequences unlikely and on the other hand the variety of targets means that mistakes in attack against single target are unlikely seen as a show-stopper in any way.

5.7 Cyber attack

5.7.1 Distributing the plan

Distributing instructions have been covered in previous chapters broadly, because Anonymous used same communication method and process for a variety of things. Actual attack plans were distributed in a similar fashion. As a summary, plan was distributed mostly via IRC topic messages. Instructions were also given at times by seemingly authoritative Anonymous members, which of whom many seemed to be administrators on the IRC server.

5.7.2 Rehearsing

Rehearsing in Grant et al. (2015) model is input for 'operatives ready', which is then followed by the cyber attacks. Rehearsing takes as input the plan that has been distributed. As was noted in 6.6.4. Testing plan, no testing or rehearsal was observed in the research material. In 6.6.4. are also discussed possible reasons for this, which won't be repeated here.

5.7.3 Penetrate & control

In Grant et al. (2015) model, penetrate & control takes as input incoming commands, ready operatives and the distributed plan. As output of the process, there are outgoing commands, C2 channel, weapons embedded, persistent control and it acts as input for violate systems process. The inputs for penetrate & control have already been discussed.

Overall, in the research no clear evidence of controlling any systems was recognized, apart from social media which is discussed later. It must be emphasized that this is not evidence implying that controlling systems did not happen. Such activity may have been discussed on other communication channels.

However, significant number of tools related to penetrating to systems and controlling them were mentioned and distributed. In the GitHub repository, 30 different attack tools were included of which 8 were backdoors used for controlling a penetrated system. There were for example db_autopwn.rb, an automated attack tool, and vbul5.pl, aVbulletin software remote code execution exploit. In the IRC discussions, several penetration capable tools were referred to. These included sqlmap, Wfuzz, WebSploit and Armitage. This implies that penetration and control of systems was attempted.

Some evidence of controlling ISIS websites and social media accounts was recorded by the media. An example of this was gay pornography and pride flags posted on ISIS twitter accounts, that had allegedly been hacked by Anonymous members (Losteminor, 2017). Another instance was a website that was breached and website was replaced with an advertisement leading to online shop selling Viagra (Mirror, 2015). Not many examples of this kind were found, and these cases documented by media are likely the most reliable evidence of results of Anonymous' efforts in penetrating & controlling ISIS systems.

5.7.4 Violate systems

In the Grant et al.'s (2015) model, violate systems takes as inputs the distributed plan, incoming commands, penetrate & control process and persistent control. Violate systems process produces as output goals achieved and log files.

As noted previously when elaborating goals of this campaign, the main goals were Denial of Service of websites and on social media. Denial of Service was the main method of system violation in the research material. Several Denial of Service tools were distributed via the GitHub repository. Several versions of SlowLoris DoS attack tool were included. Also, sockstress, a TCP protocol DoS exploit was in the repository. DoS attacks were widely discussed in the IRC conversations and there was a dedicated IRC channel for ISIS related DDoS conversations.

Like previously in reconnaissance chapter, social media-related tools are discussed here. The reason for including social media-related attack tools here instead of in the previous section is that these tools cannot be used to 'penetrate' or 'control' their targets in anyway, rather by their nature to 'violate'. Violate in this case means in practice to report the accounts to the social media platform. The goal of reporting was to take down the accounts by claiming that they contain abusive, harassing or violent content. The reasoning behind this is that terrorist supporting content should not be allowed but removed from the social media platforms.

The extent of Anonymous' success in this widespread account reporting is unclear. According to an unnamed source at Twitter interviewed by the Daily Dot (2015), the lists of ISIS affiliated accounts Anonymous has been reporting are 'wildly inaccurate'. It is probably impossible to find a better source for this kind of information given the circumstances, as only Twitter can at some rate of confidence even say which accounts have been reported by Anonymous. The tools rely mostly on jihadist keywords and single keyword hit may result in report which obviously means that there is significant amount of false positive reports, as possibly a lot of non-pro ISIS discussion included these same keywords.

That being said, the amount of reporting activity was significant judging by the discussion on IRC and amount of reporting tools distributed and without doubt these have produced results as well. Thousands of messages that had references to Twitter, Facebook and Instagram were included in the research data. From the research data, however, it is not possible to evaluate the extent or success of these operations. Media reported takedowns of thousands of Twitter accounts, as an example of these Yahoo Finance (2015) used Anonymous Twitter account as the source. This underlines the fact that it is very difficult to evaluate this type of activity with any reliability, as comprehensive and reliable data sources are not available.

5.7.5 Lessons learned

The lessons learned section that was in its entirety included under Carr's model's Cyber attack section contains processes assess damage, unintended effects and disseminate lessons learned.

Overall, only very limited amount of discussions related to any processes of lessons learned were observed in the research material. Several mentions of Denial of Service attack either working or not working were discussed. Results of Denial of Service exploits either working or not working were included in the IRC chats, but no more detailed analysis of any kind was observed. None of the gathered website materials included any thoughts or mentions about effectiveness of used methods or of any goals achieved. The discussion was very informal in general and notes of sites taken down were as well, example of this is provided below:

Dec 11 18:22:39 --> chez_novo (null@i.hope.you.step.on.a.lego.sir) has joined #OpIceISIS
Dec 11 18:23:17 <atomax> Koranensbudskap.se is DOWN, Muslimguide.se is DOWN, Islamguiden.com is DOWN, Jihadica.com is DOWN, islamic-world.net is HACKED and we at @anonswedes/ @caps_lock_crew are drunk.
Dec 11 18:24:48 <-- ArchLinux has quit (Connection closed)
Dec 11 18:25:30 <twelve> lol
Dec 11 18:25:38 --> Ghik (Free@Aken.Otherwise) has joined #OpIceISIS
Dec 11 18:25:40 <twelve> nice

Similar limited discussions on effects and damages were observed. It must be noted that when compared to initial goals, this type of discussion can be expected, as the main content of the goals was simply to take down websites and social media accounts – nothing more complicated.

6 CONCLUSIONS AND DISCUSSION

6.1 Conclusions

6.1.1 Literature review and used models

Goal of this study was to use a model of a cyber conflict to analyze one conflict in detail as a case study, using netnographic analysis of gathered research material. Carr's Cyber Early Warning Model was used to analyze the conflict between Anonymous and ISIS in 2015, from Anonymous point of view on the conflict level, and Grant et al. (2015) canonical model of offensive cyber operations from the cyber attack level. In the study, these were combined into a single model under which the analysis was done. In this conclusion chapter, first the literature review is addressed after which the results of the case study are analyzed.

The following questions were the research questions used in this study:

- How do political conflicts escalate in cyberspace to cyber attacks or warfare?
    - What are the phases of a cyberspace-based political conflict?
    - What are the actors in cyber conflicts and attacks?
    - When can a conflict in the cyberspace be called cyber warfare or terrorism?
- How do cyber attack campaigns proceed in a political conflict?
    - How and what kind of cyber attacks can be used in a political conflict?

Regarding the first question, the study concluded that the five phases of Carr's (2011) model existed also in this conflict, although in different order than the model's presupposition was. The findings were similarly slightly conflicting with Grant et al. (2015) model which had the same presupposition of phase ordering. The conflict developed on a general level in the following order:

1. Latent tensions
2. Initiating events
3. Cyber mobilization
4. Cyber reconnaissance
5. Cyber attacks.

Similarly, Grant et al.'s (2015) Canonical Offensive Cyber Operations Model was a good fit for analysis. Continuing along the same line, the model's different phases could be observed in the research material though the order of the processes differed at times.

For this kind of case study of a political cyber attack campaign, neither of the models would give enough structure to work by themselves, but as they were easily combined because the models had a similar structure, they could be used together to handle from the higher level political conflict point of view all the way to the details of the cyber attacks.

A political conflict based in the cyberspace may have different actors that can be categorized to different classes. In this study Sigholm's (2013) actors were used, and of these the following were found to be possible actors: ordinary citizens, hacktivists, patriot hackers, cyber terrorists, cyber espionage agents and cyber militias. Regarding subject actors of the case study, Anonymous and ISIS, it is hard to draw a definitive conclusion to which category they should be put into. Conclusion was to categorize Anonymous as 'hacktivist' and ISIS as 'cyber terrorist'.

Cyber warfare does not currently have a definition in any United Nations' agreements. Looking at the question another way round, judging if the persons participating would be treated as 'soldiers' as in Geneva Convention is one way to define if the acts were parts of a war. Regarding the case study and Anonymous, the participants were more likely to be judged by criminal laws. On the other hand, ISIS operatives located in the Near East warzones, could be treated as soldiers with Geneva Convention applying. From this point of view, the conflict cannot be stated to a war because Geneva Convention would not likely apply to both parties' participants, or even a majority of them. Also, the attacks are conducted by Anonymous hacktivists to whom Geneva Convention does not apply. Moreover, if Clausewitz's (1832) definition that was summarized to war being violent, instrumental and political into account, this conflict cannot be stated to be war as it was not violent. No evidence of physical harms exists in the research data.

6.1.2 Summary of the results from the case study

The latent tensions were tensions of core values of the groups and the motivation of Anonymous strongly came also from their fear of insecurity after Paris attacks. Initiating events that led to attacks was the Paris bombing on Friday evening of 13 November 2015 that was followed by the social media mobilization effort of Anonymous. Mobilization gathered very quickly hundreds of people interested in contributing in efforts against ISIS, but a large number participants obviously were not knowledgeable in cyber attacks and had only very minor contribution.

In the first phase the Anonymous insiders discouraged participants from hacking and guided them to gather intelligence about targets. The orders were to post relevant information to provided IRC channels or website drops from which the information was passed on, likely to the more skilled hackers involved. Two weeks after the start of OpParis, the

message changed from gathering intelligence to attacking and hacking all sites and social media accounts. Attack methods ranged from exploiting websites to DDoS attacks, and on social media side methods were mostly to report accounts posting violent propaganda. Also, an operation that used information operation methods was launched later, aiming to inject counter-propaganda to ISIS websites and social media profiles.

Anonymous aimed to use a variety of intelligence gathering and cyber attack methods. Intelligence gathering was fairly wide and results-oriented, but at the same time chaotic because of the loose nature of the collective. Cyber attack methods seemed to consist mostly of Denial of Service attacks and social media account takedown efforts, which was probably due to target organization likely having a very flat and simple IT infrastructure, social media included, to attack. ISIS's communications were very active in social media, which is why Anonymous' focus on social media takedown and counter-propaganda operations can be seen as logical, especially as they were automated extensively with scripts and other tools.

6.2 Limitations

The main model used, Cyber Early Warning Model, was a fairly good fit for analysis. It drawbacks were that it 1) was structured in order of a conflict between well-resourced nation-states, 2) wasn't very detailed in its sections and 3) didn't include any post-conflict analysis of the effects taking place, like compared to Kadende-Kaiser et al. (2003) presented phases of conflict, which was used as example in literature review in 2.1.2. In this case, the third wasn't a real challenge as conflict goes on by the time of writing, but the first and second are worth exploring. On the other hand, relevance of previously stated third limitations is likely to grow as cyber attacks gain popularity as methods for aggressive politics. The other model used, Grant et al.'s (2015), was similarly good fit for analysis. This model provided the necessary details that Carr's model was missing.

For a nation-state that is well resourced, the reconnaissance might happen in advance but for non-state actors and less-resourced nation-states it is more likely to happen only after initiating events have taken place. In this case, the order was rather tensions, events, mobilization, recon, and lastly attacks, meaning only two phases were in the same place as the model supposed.

The model is unlikely by itself to give ability to use it as an "early warning model" as its name states, as it is only topic level description of different sequences in a cyber-based conflict. The model needs further elaboration and work under each of its categories to produce an actual description of events, though someone could see this is also as a feature of the model as conflicts do differ a lot. Despite the previous critique of the model, it was fairly good fit for analysis as stated in the beginning. All the phases were present and it

included all the different phases the conflict took. It served as a useful framework for constructing thorough view of the conflict.

The material and the object of the study itself produced clear limitations to the study; a researcher can't be certain about truthfulness of anything seen in the material. Any comment, questions or statement might be by some actor trying to influence Anonymous. On the other hand, this leads again to the question: as anyone can be member of Anonymous by their decision in any given moment, how much does it matter? Short answer is that is does matter - if the research aims to analyze the behavior of individuals who honestly desire to contribute to the cause of Anonymous and this particular campaign. But as even a nation-state might temporarily agree with the goals and even contribute, openly or covertly, the question remains difficult to answer.

Third limitation is about the actual results of actions that were analyzed; it was impossible to determine which methods were actually used, to which extent and how successfully. Of some methods, like the social media account reporting the material clearly gave away methods used – but not how much were they used. While that would be valuable data it is also too detailed for a study that focuses on the conflict and its developments. This limitation is likely to exist in similar future studies if material is gathered of any real conflict in a similar broad setting.

Fourth limitation was the amount of data that the study produced. All the data cannot be analyzed with detailed without enormous effort and analyzing only one week worth of data would not give a good picture of the conflict. Because of this, a factor of error remains in the study findings.

6.3 Implications for further research

Future work on modeling cyber-based political conflicts is yet to be done, and based on this study especially in developing more accurate and complete frameworks for how and why conflicts take different paths. Such future model would also need a way to analyze the post-attack phase and possible social, political and legal aftermath, and effects that attacks might cause in larger picture of events, since conflicts in the cyberspace are unlikely to be isolated, but rather a side-plot in a larger political conflict or trend. This kind of more comprehensive analysis framework or model is something that should be explored further.

Of the material used in the study there are numerous possibilities for future research to be made. Just to mention few examples, the material could be analyzed sociologically or psychologically just to follow how the group's narrative develops in this conflict where everything happens online and actors are distributed around the world. Similarly, a purely technical study could be done regarding all or a subset of the technical data and methods

presented in the material. The material contains examples of exploits used and the IRC logs contain hundreds of references to exploiting and reconnaissance tools that could inspected more closely.

REFERENCES

Akyol, M. (2015). A Medieval Antidote to ISIS. http://www.nytimes.com/2015/12/21/opinion/a-medieval-antidote-to-isis.html?_r=0, retrieved 10.06.2016

Al Akhbar English (2014). What does ISIS' declaration of a caliphate mean? http://english.al-akhbar.com/node/20378, retrieved 10.04.2016

Al-Rawi, A. (2014), "Cyber warriors in the Middle-East: the case of Syrian Electronic Army". *Public Relations Review, 40(3), 420-428.*

Alkaff, S. (2015). Islamic State: Breeding a New Generation of Jihadists. *RSIS Publications, August 2015*.

Allagui, I., – Kuebler, J. (2011). The Arab Spring and the Role of ICTs| Introduction. *International Journal of Communication*, *5, 8.*

Andress, J. – Winterfield, S. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Elsevier, United States of America.

Anonymous Italy (2015). Anonymous | #OpParis [ENG]. https://www.youtube.com/watch?v=g-qGl4mVTuY, retrieved 16.04.2016

Baker, K. (2015). Hacking group Anonymous declares war on ISIS in YouTube video saying it will use its knowledge to 'unite humanity'. http://www.dailymail.co.uk/news/article-3320055/Hacking-group-Anonymous-declares-war-Isis-YouTube-video.html, retrieved 16.04.2016

BBC (2015). Ghost Security Group: 'Spying' on Islamic State instead of hacking them. http://www.bbc.com/news/blogs-trending-34879990, retrieved 01.12.2017

BBC (2003). Matrix mixes life and hacking. http://news.bbc.co.uk/2/hi/technology/3039329.stm, retrieved 28.12.2017

Besseling, K. et al. (2013). Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructure Protection, January 2013*.

Borghard, E. – Lonergan, S. (2016). Can States Calculate the Risks of Using Proxies? *Orbis, Volume 60 (3), 395-416*.

Brenner, E. – Clarke L. (2011). Conscription and Cyber Conflicts: Legal Issues. *3rd International Conference on Cyber Conflict,* eds. Czosseck, C. - Tyugu, E. & Wingfield, T. (Eds.). Tallinn, Estonia.

Brown III, H. (2016). SPCTA: An Analytical Framework for Analyzing Cyber Threats by Non-State Actors. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *6*(2), 41-60.

Carr, Jeffrey (2011). *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly Media, United States of America.

CCDCOE – NATO Cooperative Cyber Defense Centre of Excellence (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, United Kingdom.

von Clausewitz, C. (1832). *On War* (translated by J.J. Graham). Wien, Austria.

Council of Europe (2001). Details of Treaty No. 185 – Convention on Cybercrime. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, retrieved 15.03.2016

Cresswell, J. (2010). Oxford Dictionary of Word Origins. Oxford University Press, Oxford.

Cronin, A. (2015). ISIS is not a terrorist group: Why counterterrorism won't stop the latest jihadist threat. *Foreign Affairs*, 94, 87.

Daily Dot (2015). "Twitter: Anonymous's lists of alleged ISIS accounts are 'wildly inaccurate' " http://www.dailydot.com/politics/twitter-isnt-reading-anonymous-list-isis-accounts/, retrieved 11.4.2016

Damele B. & Stampar M. (2017). SQLmap introduction. http://sqlmap.org/, retrieved 25.12.2017

DeLuca, C. D. (2013). The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors. *Pace Int'l L. Rev. Online Companion*, ii. http://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1033&context=pilronline, retrieved 11.11.2017

Deibert R. – Rohozinski R. (2011). "The New Cyber Military Industrial-Complex," *Globe and Mail*, 28 March 2011.

Deutsch, M. et al. (ed.) (2011). The handbook of conflict resolution: Theory and practice, 308-311. John Wiley & Sons.

Denning, D. E. (2010). Cyber Conflict as an Emergent Social Phenomenon. Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications. IGI Global, Michigan.

Denning, D.E. (2001). Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy. *Networks and Netwars: The Future of Terror, Crime, and Militancy,* eds Arquilla J – Ronfeldt D, 239–288. Santa Monica, CA.

Dobusch, L. – Dennis, S. (2015). "Fluidity, identity, and organizationality: The communicative constitution of Anonymous." *Journal of Management Studies*, 1005-1035. 52(8).

Dombrowski, P., - Demchak, C. (2014). Cyber war, cybered conflict, and the maritime domain. *Naval War College Review*, *67*(2*), 70.*

East-West Institute (2014). Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity, Eds. Habes, B. – Andrey, K. – Kal, F. & Valery, Y. https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf, retrieved 30.3.2016

Elkus A. (2009). The Rise of Cyber Mobilization. The Ooda Loop. https://www.oodaloop.com/uncategorized/2009/02/13/the-rise-of-cyber-mobilization/, retrieved 29.2.2016

Finnish Ministry of Communications (2016), "Kyberturvallisuuden vuosiraportti 2015." https://www.viestintavirasto.fi/attachments/tietoturva/Viestintaviraston_Kyberturvallisuuskeskuksen_vuosiraportti_2015.pdf, retrieved 10.2.2016

Gartner (2017). “Gartner Says Worldwide Public Cloud Services Market to Grow 18 Percent in 2017”. https://www.gartner.com/newsroom/id/3616417, retrieved 27.07.2017

Geers, K., Kindlund, D., Moran, N., Rachwald, R. (2014). “World War C: Understanding Nation-State Motives Behind Today’s Advanced Cyber Attacks”. http://msdsrnd.com/wp-content/uploads/2016/10/fireeye-wwc-report.pdf, retrieved 29.07.2017

GhostSec – Ghost Security Research & Special Operations (2016). Our mission. http://ghostsec.org/, retrieved 11.04.2016

Ghost Security Group (2016). About. https://ghostsecuritygroup.com/, retrieved 11.04.2016

Government of South Africa (2011). A national cybersecurity policy framework for South Africa. http://www.cyanre.co.za/national-cybersecurity-policy.pdf, retrieved 30.3.2016

Grant, T. et al. (2015). "Comparing models of offensive cyber operations." *Leading Issues in Cyber Warfare and Security: Cyber Warfare and Security 2*, p. 35.

HIIK – Heidelberg Institute for International Conflict Research (2011), “The shared methodological approach, revised in 2011”. http://www.hiik.de/en/methodik/index.html, retrieved 1.3.2016

Hollis, D. (2015). Cyberwar case study: Georgia 2008. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf, retrieved 17.8.2017

Huang, J. (2015). Values and Symbolism in Anonymous’s Brand Identity. https://pdfs.semanticscholar.org/69ed/732e4eadd08418008cc3b24a70e4c040dad0.pdf , retrieved 25.11.2017

Hunker, J. et al. (2008). Role and challenges for sufficient cyber-attack attribution. http://www.scis.nova.edu/~cannady/ARES/hunker.pdf, retrieved 12.02.2018

IETF - Internet Engineering Task Force (1993). RFC 1459. https://tools.ietf.org/html/rfc1459#section-1, retrieved 10.04.2016

Illia, L. (2003). Passage to cyberactivism: how dynamics of activism change. *Journal of Public Affairs,* 3(4): 326–337.

Iltalehti (2011). F-Secure: Anonymous Finland saattoi kaataa poliisin sivut. http://www.is.fi/kotimaa/art-2000000447040.html?nomobile=4, retrieved 11.09.2017

Internet Worlds Statistics (2015). Internet growth statistics. http://www.internet-worldstats.com/emarketing.htm, retrieved 12.04.2016

IMPACT-Alliance (2016), Mission and Vision. http://www.impact-alliance.org/aboutus/mission-&-vision.html, retrieved 15.3.2016

Jones S. & Khalaf R. (2014). Selling terror: how Isis details its brutality. http://www.ft.com/cms/s/2/69e70954-f639-11e3-a038-00144feabdc0.html?%E2%80%94ftcamp=crm/email/2014617/nbe/AsiaMorningHeadlines/product, retrieved 10.04.2016

Kadende-Kaiser, R. – Kaiser, P. (2003). Phases of Conflict in Africa. *Journal of Asian and African Studies*, *38* (2-3), 150-161.

Kallberg J. – Thuraisingham, B. (2013). From Cyber Terrorism to State Actors' Covert Cyber Operations. *Strategic Intelligence Management, 2013*, 229-233.

Kissinger, H. (2014). World Order: Reflections on the Character of Nations and the Course of History. Allen Lane.

Kozinets R. (2015). "Management Netnography: Axological & Methodological Developments in Online Cultural Business Research". *The Sage Handbook of Qualitative Business & Management Research Methods*.

Kozinets, R. (2015). Netnography: Redefined. Sage, London.

Kozlowski, A. (2014), "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgystan". *European Scientific Journal,* February 2014 special edition vol.3.

Kuehl, D. (2009), "From Cyberspace to Cyberpower". Cyberpower and National Security. Eds. Kramer, F. - Starr S. & Wentz L. Potomac Press.

Liles, L. (2014). The Civilian Cyber Battlefield: Non-State Cyber Operators' Sta-tus Under the Law of Armed Conflict. *North Carolina Journal Of International Law & Commercial Regulation,* 39(4), 1091-1121.

Luiijf, E. et al. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures* 6, 9(1-2), 3-31.

Losteminor (2017). Anonymous has hacked ISIS' Twitter accounts AGAIN and made them fabulously gay. http://www.lostateminor.com/2017/05/11/isis-social-media-accounts-are-filling-up-with-gay-porn/, retrieved 30.12.2017

Manap, M. et al. (2013), Cyber terrorism challenges: The need for global response to a multi-jurisdictional crime. *Computer Law & Security review*, 23, 207-215.

Maness, R. & Valeriano, B. (2012). The Fog of Cyberwar: Why the Threat Doesn't Live Up to the Hype. https://www.foreignaffairs.com/articles/2012-11-21/fog-cyberwar, retrieved 12.02.2018

Mirror (2015). Anonymous hacks ISIS website and replaces it with Viagra advert and message to calm down. http://www.mirror.co.uk/news/world-news/anonymous-hacks-isis-website-replaces-6905409, retrieved 30.12.2017

Nash, J. (1998). Terrorism in the 20th Century: A Narrative Encyclopedia - From the Anarchists, through the Weathermen, to the Unabomber. M. Evans & Company.

Offensive Security (2017). Kali Linux Tools Listing. https://tools.kali.org/tools-listing, retrieved 23.09.2017

Orin, A. (2014). Behind the App: The Story of Kali Linux. https://lifehacker.com/behind-the-app-the-story-of-kali-linux-1666168491, retrieved 23.09.2017

Oxford Dictionaries (2017). Espionage. https://en.oxforddictionaries.com/definition/espionage, retrieved 18.08.2017

Olson, P. (2012). We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency. Hachette Digital.

Peterson, N. (2015). Hunting ISIS: We're Killing 1000 Fighters a Month. http://europe.newsweek.com/hunting-isis-were-killing-1000-fighters-month-333116?rm=eu, retrieved 06.04.2016

Rid, T. (2012)."Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 February 2012, pp. 5–32.

Rohan, S. (2017). Smart Home Market worth 137.91 Billion USD by 2023. http://www.marketsandmarkets.com/PressReleases/global-smart-homes-market.asp, retrieved 27.07.2017

Rouse, M. (2007). Definition: footprinting. http://searchsecurity.techtarget.com/definition/footprinting, retrieved 23.09.2017

Rouse, E. (2012). Psychological Operations/Warfare. http://www.psywarrior.com/psyhist.html, retrieved 01.12.2017

Ruby, C. (2002). The definition of terrorism. *Analyses of social issues and public policy*, *2*(1), 9-14.

Rummel, R.(1976). Understanding Conflict and War. Vol. 2 The Conflict Helix. http://www.hawaii.edu/powerkills/TCH.CHAP27.HTM, retrieved 02.08.2017

Ruthven, M. (2015). "Inside the Islamic State. Review of Islamic State: The Digital Caliphate by Abdel Bari Atwan". New York Review of Books.

Schmitt, M. (2012). Classification of Cyber Conflicts. *Journal of Conflict and Security Law*, Volume 17, Issue 2, 1 July 2012, Pages 245–260

Shakarian P. et al. (2013). Introduction to Cyber-Warfare: A multidisciplinary approach. Newnes.

Sigholm, J. (2013). Non-State Actors in Cyberspace Operations. *Journal of Military Studies*, *4*(1), 1-37.

Singer, P. – Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know, 110-114. Oxford University Press.

Sriram, C. – Wermester, K. (Eds.). (2003). From Promise to Practice: Strengthening UN Capacities for the Prevention of Violent Conflict. Lynne Rienner Publishers.

Stone, N. (1966). Hungary and the Crisis of July 1914. *Journal of Contemporary History*, *1*(3), 153-170.

Pollitt M.(1998). Cyberterrorism - fact or fancy?. *Computer Fraud & Security,* February 1998, 8-10.

Pruitt, D. – Kim, S. (eds.) (2004, 3rd Edition) Social Conflict, Escalation and Settlement, McGraw Hill Higher Education, New York, NY.

Slate (2011). Recognizably Anonymous logo.http://www.slate.com/content/dam/slate/articles/arts/design/2011/12/111207_DESIGN_anonymousLogo.gif.CROP.article250-medium.gif, retrieved 11.09.2017

The Atlantic (2015). The Cyber Activists Who Want to Shut Down ISIS. https://www.theatlantic.com/international/archive/2015/10/anonymous-activists-isis-twitter/409312/, retrieved 11.11.2017

The Daily Dot (2015). Twitter: Anonymous's lists of alleged ISIS accounts are 'wildly inaccurate'. https://www.dailydot.com/layer8/twitter-isnt-reading-anonymous-list-isis-accounts/, retrieved 01.12.2017

Telegraph (2015). Paris terror attack: Everything we know on Saturday afternoon. http://www.telegraph.co.uk/news/worldnews/europe/france/11995246/Paris-shooting-What-we-know-so-far.html, retrieved 15.04.2016

Traynor, I. (2015). EU ministers order tighter border checks in response to Paris attacks. http://www.theguardian.com/world/2015/nov/20/eu-ministers-order-tighter-border-checks-in-response-to-paris-attacks, retrieved 15.04.2016

Valentino-Devries, J. – Yadron, D. (2015). Cataloging the World's Cyberforces. http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710, retrieved 20.3.2016

Ventre, D. (2011). Cyberwar and Information Warfare. Wiley-ISTE, UK.

United Nations (2013). Security Council Al-Qaida Sanctions Committee Amends Entry of One Entity on Its Sanctions List. http://www.un.org/press/en/2013/sc11019.doc.htm, retrieved 29.1.2016

United Nations (1994). Measures to eliminate international terrorism. http://www.un.org/documents/ga/res/49/a49r060.htm, retrieved 12.2.2018

US State Department (2016), Foreign Terrorist Organizations. http://www.state.gov/j/ct/rls/other/des/123085.htm, retrieved 29.1.2016

Yahoo Finance (2015). Hackers vs terrorists: Over 6000 ISIS Twitter accounts taken down. https://finance.yahoo.com/news/hackers-vs-terrorists-over-6-000-isis-twitter-124536524.html, retrieved 1.1.2018

Youth Department of the Council of Europe (2017). Counter Messaging: Occupying Public Space. http://www.bg06eeagrants.bg/sites/default/files/WeCANmanual_FINAL_MAJ17032017.pdf.pdf, retrieved 01.12.2017

Wheeler, D. – Larsen, G. (2003). Techniques for cyber attack attribution. Institute for Defense Analyses, VA.

Wikipedia (2012). A contemporary Guy Fawkes mask. https://en.wikipedia.org/wiki/Guy_Fawkes_mask#/media/File:GuyFawkesMask.jpg, retrieved 11.09.2017

Wikipedia (2013). Flag of the Islamic State. https://en.wikipedia.org/wiki/Islamic_State_of_Iraq_and_the_Levant#/media/File:AQMI_Flag_asymmetric.svg, retrieved 11.09.2017

Winokoor, C. (2011). Military enlistment got boost as result of 9/11 terror attacks. http://www.tauntongazette.com/x1638743381/INSPIRED-ACTION-9-11-tragedy-turns-to-drive-for-recruits, retrieved 23.09.2017

Winter, C. (2015). Documenting the Virtual Caliphate. http://www.quilliaminternational.com/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf, retrieved 20.9.2017

Zelin, A. (2014). The War between ISIS and al-Qaeda for Supremacy of the Global Jihadist Movement. http://www.washingtoninstitute.org/uploads/Documents/pubs/ResearchNote_20_Zelin.pdf, retrieved 06.04.2016

APPENDICES

Appendix 1: Known offensive cyber capabilities of nation-states.

Country	Goals	Targets	Software	Misc
Argentina	Surveillance	?	Developed	Interest in offense and defense
Australia	Surveillance	Domestic, int.	Developed, purchased	
Azerbaijan	Surveillance	Domestic	Purchased	Motivation in anti-activism
Bahrain	Surveillance	Domestic, int.	Purchased	
Bangladesh	Surveillance, defacement	Domestic, int.	Purchased	Using private teams
Belarus	National security	?	?	
Belgium	Surveillance	?	Purchased	
Bosnia and Herzegovina	Surveillance	?	Purchased	
Brazil	Surveillance	Domestic	Purchased	
Bulgaria	Surveillance	?	Purchased	-
Canada	Surveillance	Domestic, int.	Developed	Snowden documents indicate attack capabilities
Chile	Surveillance	Domestic	Purchased	
China	Surveillance, defacement	Domestic, int.	Developed	Capability for attacks
Colombia	Surveillance	Domestic	Developed, purchased	
Cyprus	Surveillance, national security	?	Purchased	
Czech Republic	Surveillance	Domestic	Purchased	Stated to be only for police action

Denmark	Defensive and offensive capability	?	Developed	Significant offensive program
Ecuador	Surveillance	Domestic	Purchased	Associated with hacker group Hacking Team
Egypt	Surveillance	Domestic	Purchased	Anti-activism
Estonia	Surveillance, national security, 1, 2	?	Purchased	Volunteer group Cyber Defense Unit
Ethiopia	Surveillance	Domestic, int.	Purchased	
Finland	Defensive and offensive capability	?	Developed	
France	Surveillance, defensive and offensive capability	International	Developed	
Germany	Surveillance	Domestic, int.	Developed, purchased	
Honduras	Surveillance	?	Purchased	Anti-activism suspected goal
Hungary	Surveillance	International	Purchased	Domestic use unclear
India	Surveillance, defacement,	International	Developed	Developing offensive capabilities
Iran	Surveillance, defacement, destruction	Domestic, int.	Developed	Significant offensive capabilities
Israel	Surveillance, destruction	Domestic, int.	Developed	Advanced spying capabilities
Italy	Surveillance	Domestic, int.	Developed, purchased	
Kazakhstan	Surveillance	?	Purchased	
Lebanon	Surveillance	Domestic, int.	Developed, purchased	

Luxembourg	Surveillance	Domestic	Purchased	For police operations
Malaysia	Surveillance	?	Purchased	
Mexico	Surveillance	Domestic, int.	Purchased	
Mongolia	Surveillance	?	Purchased	
Morocco	Surveillance	Domestic	Purchased	Hints of anti-activism
Myanmar	Surveillance, defacement	Domestic, int.	?	Publicly stated mission of network-centric warfare, anti-activism
Netherlands	Surveillance	?	Purchased, developed	
New Zealand	Surveillance	International	Developed	Helped US spy on China according to Snowden documents
Nigeria	Surveillance	Domestic	Purchased	
North Korea	Surveillance, destruction	International	Developed	Significant offensive personnel, domestic use unclear
Norway	National security	?	Developed	Preparing offensive cyberweapons
Oman	Surveillance	?	Purchased	
Pakistan	Surveillance, defacement	Domestic, int.	Developed, purchased	Suspected of using private groups, of cyberespionage.
Panama	Surveillance	Domestic	Purchased	Purchased equipment from Hacking Team
Philippines	Surveillance	International	Developed	
Poland	Surveillance	Domestic	Developed, purchased	Military strategy aims for both offense and defense
Qatar	Surveillance	?	Developed, purchased	

Russia	Surveillance, defacement, destruction	Domestic, int.	Developed, purchased	Advanced capabilities in malware
Saudi Arabia	Surveillance	Domestic	Purchased	
Singapore	Surveillance	?	Purchased	
South Africa	Surveillance	Domestic	Developed, purchased	
South Korea	Surveillance	Domestic, int.	Developed, purchased	Announced development of offensive capabilities
Spain	Surveillance	International	Developed, purchased	
Sudan	Surveillance	?	Purchased	Targets unclear
Switzerland	Surveillance	?	Developed, purchased	
Syria	Surveillance, defacement	Domestic, int.	Developed	Using private groups, anti-activism
Thailand	Surveillance	International	Purchased	Denied domestic use
Turkey	Surveillance	Domestic, int.	Purchased	Military has "Cyber Warfare Command"
Turkmenistan	Surveillance	?	Purchased	Government servers found running hacking software
UAE	Surveillance	Domestic	Purchased	Anti-activism
UK	Surveillance, 2, 3	Domestic, int.	Developed	
Ukraine	Surveillance, defacement	International	?	Using private groups
USA	Surveillance, destruction, 1	Domestic, int.	Developed, purchased	Advanced capabilities in offensive operations
Uzbekistan	Surveillance	?	Purchased	
Vietnam	Surveillance, defacement	Domestic, int.	Developed, purchased	Using private groups. Allegedly

				used malware in domestic spying

Table 6 Known offensive cyber capabilities of nation-states (Valentino-Devries & Yadron, 2015)

Appendix 2: International legislation regarding cyber terrorism

Manap et al. (2013) identified the following laws and international agreements that touch the concept of cyber terrorism:

- 1963 Convention on Offences and Certain Other Acts Committed on Board Aircraft,
- 1970 Convention for the Suppression of Unlawful Seizure of Aircraft,
- 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft, 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation,
- 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons,
- 1979 International Convention against the Taking of Hostages,
- 1980 Convention on the Physical Protection of Nuclear Material,
- 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation,
- 1989 Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation,
- 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation,
- 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation,
- 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf,
- 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection,
- 1997 International Convention for the Suppression of Terrorist Bombings,
- 1999 International Convention for the Suppression of the Financing of Terrorism,
- 2005 International Convention for the Suppression of Acts of Nuclear Terrorism, and
- 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation

Appendix 3: Parts of the Canonical Offensive Cyber Operations Model

In this appendix the details of the canonical offensive cyber operations model by Grant et al. (2015) The model parts have been put into a list form so that notes regarding their content can be added easily. In any given part, the factors that are the processes have been bolded. Word 'both' is used to mean 'both input and output'. All parts of the model contain one or more factors that are processes.

The first step of the model is 'Select goals'.

Factor	Input / Output / Process	Note
1. Incoming cyber attack	Input for 6.	Grant et al. model assumes a cyber-based adversarial context. In this study, other motivations for action are assumed to possible.
2. Incoming cyber threat	Input for 6.	Grant et al. model assumes a cyber-based adversarial context. In this study, other motivations for action are assumed to possible.
3. Authorities	Input for 6.	Grant et al. model is presented as if the actor was a government.
4. Legal advisors	Input for 6.	See above.
5. Legal compliance	Input for 6.	See above.
6. Select goals	Process; Input for 7., 8. & 9	
7. Target organization	Output	
8. Attack goal	Output	
9. Desired effects (CIA)	Output	CIA = Confidentiality, Integrity, Availability.

Table 7 Canonical model of offensive cyber operations: select goals phase

The second step is 'Select targets', which focuses on target selection. In the model, this phase is assumed to conducted by 'intelligence analysts'.

Factor	Input / Output / Process	Note
1. Attack goals & desired effects	Input for 4., 7., 8. & 11.	From previous phase.

2. Organisations	Input for 4.	Personnel.
3. Authorise intelligence collection	Input for 4.	
4. Footprint organisations	Process; Input for 5.	
5. Footprinting information	Both; Input for 7.	Information about systems and people.
6. Normal operations or systems	Input for 7.	
7. Recce system(s)	Process; Input for 8. & 9.	Recce = reconnaissance
8. Topology & access paths	Both; Input for 9.	
9. Target list	Process; Input for 10.	Note: the process of gathering target list
10. Target list	Output	Note: the end result, a list of targets.
11. Identify Vulnerabilities	Process; Input for 12.	
12. HW/SW vulnerabilities	Output	HW = hardware, SW= software

Table 8 Canonical model of offensive cyber operations: select targets phase

Third step of the model is 'Planning'. This step is assumed in the model to be responsibility of 'planners'.

Factor	**Input / Output / Process**	**Note**
1. Attack goal & desired effects	Input	From first step
2. Target list	Input	From second step
3. HW/SW vulnerabilities	Input	From second step
4. Authorise planning	Input	
5. Plan attack	Process; Input for 6. and 7.	The attack planning process
6. Resource specifications	Both; Input for 8.	
7. Attack plan	Both; input for 10.	
8. Prepare resources	Process; Input for 9. and 10.	
9. Deliverable weapons	Both; Input for 10.	

10. Test plan	Process; input for 11.,12. and 13.	
11. Plan improvements	Both; Input for 5.	
12. Resource improvements	Both; Input for 5.	
13. Tested plan	Output	

Table 9 Canonical model of offensive cyber operations: planning phase

The fourth step of the model is 'Attack'. This step is assumed to be conducted by 'operatives'.

Factor	Input / Output / Process	Note
1. Tested plan	Input for 4.	From third step
2. Authorise attack	Input for 4.	
3. Deliverable weapons	Input for 4.	From third step
4. Distribute plan	Process; Input for 5., 6. and 7.	
5. Weapons distributed	Output of 4.	
6. Plan distributed	Both; Input for X, Y and Z	
7. Operatives briefed	Both; input for 8.	
8. Rehearse	Process; Input for 9.	
9. Operatives ready	Both; Input for 10.	
10. Penetrate & control	Process; Input for X, Y, Z and K.	
11. Commands (incoming)	Input for 10. and 16.	
12. Weapons embedded	Output	
13. C2 channel	Output	
14. Commands (outgoing)	Output	
15. Persistent control	Both; Input for 16.	
16. Violate system(s)	Process; Input for 17. and 18.	
17. Goals achieved	Output	
18. Log files	Output	

Table 10 Canonical model of offensive cyber operations: attack phase

The last step of the model is ‘Lessons learned’. This step is assumed to be conducted by ‘professional group’.

Factor	Input / Output / Process	Note
1. Attack goal & desired effects	Input for X and Y	From first step
2. Tested plan	Input for 5.	From third step
3. Effects	Input for 5.	Supposedly effects from cyber attacks conducted during fourth step
4 Authorise evaluation	Input for 5.	
5. Unintended effects	Process; Input for 6.	Unintended effects evaluation process and activities
6. Unintended effects	Both; Input for 7.	The information about unintended effects
7. Assess damage	Process; Input for 9.	
8. Observable damage	Input for 7.	
9. Damage assessment	Both; Input for 10.	
10. Evaluate operations	Process; Input for 14. and 15.	
11. Operations event-log	Input for 7.	
12. Plan distributed	Input for 7.	From fourth step
13. Weapons distributed	Input for 7.	From fourth step
14. Archived information	Output	
15. Evaluation report	Both; Input for 16.	
16. Disseminate LLs	Process; Input for 18.	LL = lessons learned
17. Previous evaluation reports	Input for 16.	
18. LLs	Output	LL = lessons learned

Table 11 Canonical model of offensive cyber operations: lessons learned phase

Appendix 4: Tools Employed in the Campaign

In this first table, tools in the Github code repository of the campaign are listed, categorized and described briefly:

Name	Short description	Category
arabic.translation.2.ghost	Arabic translator	Recon
Arithmetico	Unclear, possibly username acquisition from social media	Recon
bitflip.cloudflare.py	Cloudflare resolver	Recon
captaincode.py	Twitter account name retriever	Recon
codezero.py	Twitter account triage	Recon
bindtty.c	C-written reverse shell	Attack
cloudflare.py	Cloudflare protected site enumerator	Recon
db_autopwn.rb	Metasploit based automated attack tool	Attack
dbd	Netcat clone with backdooring and encryption features	Attack
device-pharmer	Shodan API tool for checking IPs for more info	Recon
HoneyPy	Honeypot	Recon
ibrute	AppleID bruteforce tool	Attack
icmptunnel	ICMP-based C2 tool	Attack
kaiten.c	IRC based DDoS tool	Attack
katoolin	Install Kali Linux tools on another Linux distro	Misc
makeproxy	SOCKS proxy finder	Recon
mitmproxy	A mitm attack tool	Attack
perl-backdoor	Perl-written backdoor	Attack
PowerCat	Powershell-written version of Netcat	Attack
proftpd	Metasploit based FTP backdoor	Attack
proxycheck.py	Proxy keep-alive checking, unclear	Misc
pupy	Backdoor	Attack
pwnbin	Pastebin keyword crawler	Attack
pyLoris	DoS tool	Attack
/resources	Huge amount of fuzzing lists, passwords and backdoors, judging from the content, from SecLists and/or FuzzDB	Misc
sbd	SSH based backdoor	Attack

shell.php	PHP webshell	Attack
shellshock.smtp.py	SMTP Shellshock exploit	Attack
sl1 (also slowloris and slow-loris-dos)	SlowLoris DoS exploit	Attack
socat	Socat backdoor tool	Attack
sockstress	TCP protocol DoS exploit	Attack
ssh_0day	Unclear	Misc
/static-binaries	Binaries of common Linux tools, including nmap, make, tcpdump, xxd etc	Misc
Subbrute	Sub-domain bruteforcing tool	Recon
tcp_pty_shell_handler.py	A python-written backdoor	Attack
TCP-32764	A backdoor tool	Attack
tmap.py	Port scanning tool that uses TOR by design	Recon
vbul5.pl	Vbulleting RCE exploit	Attack
wifijammer	WiFi jamming tool	Attack
Wiley.The.Shellcoders.Handbook.2nd.Edition.Aug.2007.pdf	Pirated Shellcoder's Handbook	Misc
facebookreporter.py	Facebook version of widely employed Twitter Reporter	Attack
find.webservers.py	Web-server locator	Recon
flagfinder.beta.py	ISIS flag recognizer tool, based on CVS framework	Recon
goran.nmap.scan1.txt	Nmap scan results	Recon
/hackingschool	Directory including hacking lessons	Misc
hashtag.py	Twitter hashtag scanning tool	Recon
hashtags.txt	ISIS related hashtag listing	Recon
iraqi.ssh.first.10k.json.gz	Iraqi SSH server scan (possibly ASN based information)	Recon
iraqi.ssh.servers	Iraqi SSH server listing	Recon
isdruption.py	Google crawler	Recon
isis.isp.long.txt	Assumed ISIS ISP IP ranges	Recon
isis.isp.txt	Assumed ISIS area IP subnets	Recon
isis.keywords.txt	ISIS keyword list	Recon
/IsisWebSpider	A spider employing /flagfinder	Recon
isplist.txt	Assumed ISIS ISP IP ranges	Recon
ISruption.py	Google crawler, seems to be duplicate	Recon

netis.router.txt	Netis Realtek router vulnerability	Recon
noobguide.txt	Beginner guide? Includes Twitter reporter and other tools	Misc
onionslice.sh	Reverse shell designed for TOR	Attack
pastebin.search.py	Pastebin keyword crawler	Recon
peterpunk.ISIS.keyword.list.txt	ISIS keyword list	Recon
Scroll-N-Get	Twitter account reporter	Attack
shodan-search	Shodan API tool for checking IPs for more info	Recon
snoeper.py	Web-server locator	Recon
socialmediabot	ISIS social media account locator	Recon
superscan.sh	Masscan & Nmap automatic scanner, kind of wrapper	Recon
syrian.webservers.txt	Assumed scan results for finding Syrian web servers	Recon
telnet	Scan results from open telnet port scan	Recon
tr6.py	Twitter Auto-Reporter 6.0	Attack
tscope	Twitter data retriever	Recon
TwitPort	Twitter botnet tool	Attack
twitter.tags.py	Twitter account name retriever	Recon
twitteraccountscanner.py	Twitter account name retriever	Recon
twitterbot.js	Twitter user tweet & geolocation retriever	Recon
twitterfollowerslistgenerator	Twitter followers account name retriever	Recon
twitterhashtagspammer.py	Twitter hashtag spamming tool	Attack
twitterlogin.py	Twitter login with Python?	Misc
twitterreporter.py	Twitter Reporter 1.0.3.	Attack
url.list.verification.py	ISIS assocation verification helper tool	Recon
/whitevillian	ISIS website and Twitter account locator	Recon

Table 12 Tools included in the OpParis Github repository

Below in the second table are tools that come with Kali Linux with counted mentioned in the IRC chats. A summary of the data is here:

- Information gathering: 14 / 11,7%
- Vulnerability analysis: 31 / 26,1%
- Exploitation tools: 22 / 18,5%

- Forensics tools: 0 / 0%
- Web applications: 52 / 43,7%
- Stress testing: 0 / 0%

Information Gathering		**Vulnerability Analysis**		**Exploitation Tools**		**Forensics Tools**		**Web Applications**		**Stress Testing**	
TOTAL	14	TOTAL	31	TOTAL	22	TOTAL	0	TOTAL	52		
acccheck	0	BBQSQL	0	Armitage	1	Binwalk	0	apache-users	0	DHCPig	0
ace-voip	0	BED	0	Backdoor Factory	0	bulk-extractor	0	Arachni	0	FunkLoad	0
Amap	0	cisco-auditing-tool	0	BeEF	0	Capstone	0	BBQSQL	0	iaxflood	0
Automater	0	cisco-global-exploiter	0	cisco-auditing-tool	0	chntpw	0	BlindElephant	0	Inundator	0
bing-ip2hosts	0	cisco-ocs	0	cisco-global-exploiter	0	Cuckoo	0	Burp Suite	0	inviteflood	0
braa	0	cisco-torch	0	cisco-ocs	0	dc3dd	0	CutyCapt	0	ipv6-toolkit	0
CaseFile	0	copy-router-config	0	cisco-torch	0	ddrescue	0	DAVTest	0	mdk3	0
CDP-Snarf	0	DBPwAudit	0	Commix	0	DFF	0	deblaze	0	Reaver	0
cisco-torch	0	Doona	0	crackle	0	diStorm3	0	DIRB	0	rtpflood	0
Cookie Cadger	0	DotDotPwn	0	exploitdb	1	Dumpzilla	0	DirBuster	3	SlowHTTPTest	0
copy-router-config	0	HexorBase	0	jboss-autopwn	0	extundelete	0	fimap	0	t50	0
DMitry	0	Inguma	0	Linux Exploit	0	Foremost	0	FunkLoad	0	Terminator	0

				Sug-gester							
dnmap	0	jSQL	0	Maltego Teeth	0	Galleta	0	Gobuster	0	THC-IPV6	0
dnsenum	0	Lynis	0	Metasploit	3	Guymager	0	Grabber	0	THC-SSL-DOS	0
dnsmap	0	Nmap	14	Router-Sploit	0	iPhone Backup Analyzer	0	jboss-autopwn	0		
DNSRecon	0	ohrwurm	0	SET	0	p0f	0	joomscan	0		
dnstracer	0	Oscanner	0	ShellNoob	0	pdf-parser	0	jSQL	0		
dnswalk	0	Power-fuzzer	0	sqlmap	17	pdfid	0	Maltego Teeth	0		
DotDotPwn	0	sfuzz	0	THC-IPV6	0	pdgmail	0	PadBuster	0		
enum4linux	0	SidGuesser	0	Yersinia	0	peepdf	0	Paros	0		
enumIAX	0	SIPArmyKnife	0			RegRipper	0	Parsero	0		
Faraday	0	sqlmap	17			Volatility	0	plecost	0		
Fierce	0	Sqlninja	0			Xplico	0	Power-fuzzer	0		
Firewalk	0	sqlsus	0					ProxyStrike	0		
fragroute	0	THC-IPV6	0					Recon-ng	0		
fragrouter	0	tnscmd10g	0					Skipfish	0		
Ghost Phisher	0	unix-privesc-check	0					sqlmap	17		
Go-Lismero	0	Yersinia	0					Sqlninja	0		
goofile	0							sqlsus	0		

hping3	0							ua-tester	0		
ident-user-enum	0							Uniscan	1		
InTrace	0							Vega	21		
iSMTP	0							w3af	1		
lbd	0							Web-Scarab	0		
Maltego Teeth	0							Webshag	0		
masscan	0							Web-Slayer	0		
Meta-goofil	0							Web-Sploit	1		
Miranda	0							Wfuzz	1		
nbtscan-unixwiz	0							WPScan	6		
Nmap	14							XSSer	1		
ntop	0							zaproxy	0		
p0f	0										
Parsero	0										
Recon-ng	0										
SET	0										
smtp-user-enum	0										
snmp-check	0										
SPARTA	0										
sslcaudit	0										
SSLsplit	0										
sslstrip	0										
SSLyze	0										
THC-IPV6	0										
theHar-vester	0										

TLSSLed	0										
twofi	0										
URLCrazy	0										
Wireshark	0										
WOL-E	0										
Xplico	0										

Table 13 Tools used by category

Appendix 5: Index of gathered materials shared in IRC

In the tables below are the indexed materials that were gathered from the IRC channels. Column ‘w’ refers to number of material gathering week, starting from 17.11.2015. Column ‘doc’ is document name (as stored in the research process) which contains the title of the HTML and possibly some other indexing markers used in the research. ‘Detail’ column contains short description, in which ‘unchanged’ marker is added when same document appears again but has remained unchanged.

	1 - LATENT TENSIONS	
w	**doc**	**detail**
5	motivation-by87w - Ghostbin	Motivational infographic

	2 - INITIATING EVENTS	
w	**doc**	**detail**
1	151118-frenchpressrelease - Pastebin.com	French press release in pastebin
8	OpParis NEXT [Video] - Pastebin.com	Index of Anonymous call to action videos

	3 - RECON	
w	**doc**	**detail**
1	151118-dmitry's selection of assorted goatfags MK II - Pastebin.com	Twitter target acquisition guide
1	151118-reportingpage-OpIceISIS	IceISIS target database site created
1	151119-Df1jcUJNXZAh _ Riseup Pad	Twitter targets
1	151119-etherpad-mozilla.org/p/optakedownisis	Team division, orders + some intel
1	151119-piratepad.net/1N54kFuJgJ	Huge broad target list, copied instructions from etherpad?
1	151121-longmultitargetlist-#FUCKISIS2015 #OpParis - Pastebin.com	Target list

1	151121-ISIS MEMBER INSTAGRAM_ https___www.instagram.com_shahriyar_a13_ First picture c - Pastebin.com	Possible targets
1	20151118-opparis _ Etherpad	Targets - note falses, including cent-com.mil addresses
1	151123-qdvjx - Ghostbin	target list
2	http___alemara1.org http___alfurq4n.org http___alqassam.ps http___alsomod-i - Pastebin.com	long http & social media target list
2	ISIS MEMBER INSTAGRAM_ https___www.instagram.com_shahriyar_a13_ First picture c - Pastebin.com	possible instagram target
2	keywordlist-s5xty - Ghostbin	keywords for intel gathering
3	ISIS MEMBER INSTAGRAM_ https___www.instagram.com_shahriyar_a13_ First picture c - Pastebin.com	possible instagram target, unchanged
3	keywordlist-87wpe - Ghostbin	Revised Arabic keyword list
3	operationisil-scan-43kor - Ghostbin	Nmap results from few jihadist sites
3	piratepad-operationisil	OperationIsil pad, index of vulnerability scans
3	targetlist- Pastebin.com	target list
3	targets-22djn - Ghostbin	short target list
4	targets-22djn - Ghostbin	short target list
4	keywordlist-87wpe - Ghostbin	Arabic keywords, unchanged
4	e4udj - Ghostbin	Guide for recon; damage control
4	http___alemara1.org http___alfurq4n.org http___alqassam.ps http___alsomod-i - Pastebin.com	long http & social media target list, unchanged
4	ISIS MEMBER INSTAGRAM_ https___www.instagram.com_shahriyar_a13_ First picture c - Pastebin.com	possible instagram target, unchanged
5	targets-22djn - Ghostbin	short target list

5	2fqcg - Ghostbin	Vuln scan result of 22djn targets
5	e4udj - Ghostbin	Guide for recon; damage control
6	piratepad.net/FTG6N0mVG4	OperationIsil pad, index of vulnerability scans
6	http___alemara1.org http___alfurq4n.org http___alqassam.ps http___alsomod-i - Pastebin.com long http & social media target list, unchanged	long http & social media target list, unchanged
6	targetlist-22djn - Ghostbin	short target list, unchanged since 20.11.
7	piratepad.net/FTG6N0mVG4	OperationIsil pad, index of vulnerability scans
7	piratepad.net/tLGMVSJV0S	OpBashDaesh target list
7	targetlist-22djn - Ghostbin	short target list, unchanged since 20.11.
7	http___alemara1.org http___alfurq4n.org http___alqassam.ps http___alsomod-i - Pastebin.com long http & social media target list, unchanged	long http & social media target list, unchanged
8	http___alemara1.org http___alfurq4n.org http___alqassam.ps http___alsomod-i - Pastebin.com long http & social media target list, unchanged	long http & social media target list, unchanged
8	piratepad.net/FTG6N0mVG4	OperationIsil pad, index of vulnerability scans
8	piratepad.net/tLGMVSJV0S	OpBashDaesh target list
8	keywords-ghostbin.com/paste/4jhzw	Updated keyword list
8	targetlist-22djn - Ghostbin	short target list, unchanged since 20.11.
8	verification-ghostbin.com/paste/e4udj	target verification guide

8	Target Recommendations _ #opBashDaesh	OpBashDaesh target choosing guide
8	Tips to Finding Daesh Websites _ #opBashDaesh	OpBashDaesh target acquisition guide

	4 - MOBILIZATION	
w	**doc**	**detail**
1	151118-frenchpressrelease - Pastebin.com	French press release in pastebin
1	151119-Anonymous Action Guide #1 - Pastebin.com	Detailed action guide
1	151119-etherpad-mozilla.org/p/optakedownisis	Team division, orders + some intel
1	151119-Hunting - Pastebin.com	High level instructions
1	151121-HowToHelp - Pastebin.com	Newcomer how to help guide
2	96tdd - Ghostbin	general instructions, guide to channels
2	889gh - Ghostbin	intel gathering guide "hunting"
2	Action Guide	No changes
2	hunting	No changes
2	combat index	first revision, meta level index of resources
2	OpNewBlood	newcomer general anonymous info
2	OpParisFR - Pastebin.com	French press release in pastebin
2	q3swv - Ghostbin	Newcomer how to help guide, no changes
2	Security Handbook	Newcomer general security advice
2	VPNs	Newcomer VPN security guide
3	Anonymous Action Guide #1 - Pastebin.com	Detailed action guide, unchanged
3	Hunting - Pastebin.com	intel gathering guide "hunting", unchanged
3	hunting-889gh - Ghostbin	duplicate of above
3	hunting2-96tdd - Ghostbin	general instructions, guide to channels, unchanged
3	OpParis-Dev Official Paste-m8qjf - Ghostbin	Dev instructions, first revision
3	riseup-opparis	OpParis RiseUp pad - includes instructions in various language + some target lists
3	riseup-opparisfr	similar in French

3	uxv42 - Ghostbin	Combat index, updated
4	hunting2-96tdd - Ghostbin	general instructions, guide to channels, unchanged
4	gkjtf - Ghostbin	OpBashDaesh info-campaign first instructions
4	Hunting - Pastebin.com	intel gathering guide "hunting", unchanged
4	OpParis-Dev Official Paste-m8qjf - Ghostbin	Dev instructions, unchanged
4	opparis_intel	General intel work instructions
4	pad.riseup.net/p/opparis	OpParis RiseUp pad - includes instructions in various language + some target lists
4	public.etherpad-mozilla.org/p/optakedownisis	OpTakeDownIsis general instr + targets
4	uxv42 - Ghostbin	Combat index, updated
5	Anonymous Action Guide #2 - Pastebin.com	Motivational text & high-level strategy
5	Hunting - Pastebin.com	intel gathering guide "hunting", unchanged
5	gkjtf - Ghostbin	OpBashDaesh info-campaign, revised
5	riseup-opparis	OpParis RiseUp pad - includes instructions in various language + some target lists
5	riseup-opparisfr	similar in French
5	opparisdev-m8qjf - Ghostbin	OpParis-dev paste
5	uxv42 - Ghostbin	Combat index, unchanged
6	#opTools OVERVIEW - Generation 3 draft 1 - Pastebin.com	Botnet participation instructions
6	Anonymous Action Guide #2 - Pastebin.com	Motivational text & high-level strategy
6	Hunting - Pastebin.com	intel gathering guide "hunting", unchanged
6	hunting-889gh - Ghostbin	duplicate of above
6	index-uxv42 - Ghostbin	Combat index, updated - note ISIS opsec + hacking guide added
6	OpParis-Dev Official Paste-m8qjf - Ghostbin	Dev instructions, unchanged
6	OpParisFR - Pastebin.com	French press release in pastebin
7	#opTools OVERVIEW - Generation 3 draft 1 - Pastebin.com	Botnet participation instructions
7	Anonymous Action Guide #2 - Pastebin.com	Motivational text & high-level strategy

7	Hunting - Pastebin.com	intel gathering guide "hunting", unchanged
7	index-uxv42 - Ghostbin	Combat index, unchanged
7	OpParis-Dev Official Paste-m8qjf - Ghostbin	Dev instructions, unchanged
7	OpParisFR - Pastebin.com	French press release in pastebin
8	#opBashDaesh _ Fight ISIS Recruitment	OpBashDaesh info + recruitment for participants call to actions
8	#opTools OVERVIEW - Generation 3 draft 1 - Pastebin.com	Botnet participation instructions
8	Anonymous Action Guide #2 - Pastebin.com	Motivational text & high-level strategy, unchanged
8	combatindexfrench-yaomk - Ghostbin	French version of combat index
8	dictionary-ghost-bin.com/paste/xjwmw	Anon dictionary
8	helpguide-ghost-bin.com/paste/q3swv	Newcomer how to help guide, no changes
8	Hunting - Pastebin.com	intel gathering guide "hunting", unchanged
8	index-uxv42 - Ghostbin	Combat index, unchanged
8	noobguide-ghost-bin.com/paste/jrr89	Newcomer guide
8	OpParisFR - Pastebin.com	French press release in pastebin
8	riseup-opparis	OpParis RiseUp pad - includes instructions in various language + some target lists
8	tools-ghost-bin.com/paste/kdbey	OPSEC tools guide
8	videoguidelines-ghost-bin.com/paste/n2mq7	Guideline for Anonymous videos
8	Is Your Stupidity Helping Terrorists __ #opBashDaesh	OpBashDaesh opsec instructions

	5 - CYBER ATTACK	
w	**doc**	**detail**
1	151119-[WEBSITE AND LINKS] ========== ========== - Pastebin.com	target list including vuln
1	151119-[Python] TwitterReport (v.1.0.3) - Pastebin.com	first version of Twitter reporter

1	REDCULT	RedCult group 23k accounts taken down
1	First-week-technical materials	DDoS Guide, SQLMap, Vulscan, PHP exploit, Shell-shock, Twtter, Image recognition
2	bobtk - Ghostbin	Twitter botnet user guide, Ant-Man
2	s8bxn - Ghostbin	DDoS Guide & active target list
2	twitter-reporter-tutorialjos9g - Ghostbin	Twitter reporter tutorial
3	[Python] TwitterReport (v.1.0.3) - Pastebin.com	Twitter reporter, unchanged
3	151202-phprootinject-treuu - Ghostbin	PHP exploit
3	Anonymous - Learn Arabic - FUCK ISIS - Pastebin.com	Arabic learning materials
3	ddos-s8bxn - Ghostbin	DDoS Guide & active target list, unchanged
3	scrollnget-k6r7r - Ghostbin	Scroll n Get Twitter account retriever
3	twitport-bobtk - Ghostbin	TwitPort Twitter reporter botnet
3	TWITTER AUTOREPORTER 5.0pjuox - Ghostbin	OpIceISIS Twitter autoreporter
3	Windows Twitter Bot - Pastebin.com	Windows Twitter autoreporter
4	[Python] TwitterReport (v.1.0.3) - Pastebin.com	Twitter reporter, unchanged
4	Anonymous - Learn Arabic - FUCK ISIS - Pastebin.com	Arabic learning materials
4	twitport-bobtk - Ghostbin	TwitPort Twitter reporter botnet, unchanged
4	http///pirate-pad.net/ep/pad/view/ro.8KwRqsx$o08/latest	OpBashDaesh content for information operation

4	jos9g - Ghostbin	Twitter reporter, revised
4	scrollnget-k6r7r - Ghostbin	Scroll n Get Twitter account retriever
4	opparis_hackingschool at master · kernelzero-day_opparis	Github Hacking School for OpParis
4	pjuox - Ghostbin	Twitter autoreporter 5.0
4	s8bxn - Ghostbin	DDoS Guide & active target list, unchanged
4	vhdjs - Ghostbin	Twitter accounts from hashtags
4	Windows Twitter Bot - Pastebin.com	Windows Twitter autoreporter
4	z74o5 - Ghostbin	Twitter followers retriever
5	[Python] TwitterReport (v.1.0.3) - Pastebin.com	Twitter reporter, unchanged
5		
5	#opisis - Generation 2 BotNet Documentation - Pastebin.com	Botnet & tools documentation
5	ddos-s8bxn - Ghostbin	DDoS Guide & active target list, unchanged
5	propaganda-http///piratepad.net/5Fk0Ew0pNg	OpBashDaesh content for info-op, revised
5	[Python] TwitterReport (v.1.0.3) - Pastebin.com Twitter reporter, updated instructions	
5	z74o5 - Ghostbin	Twitter followers retriever
5	vhdjs - Ghostbin	Twitter accounts from hashtags
6	[Python] TwitterReport (v.1.0.3) - Pastebin.com Twitter reporter, unchanged	
6	#opisis - Generation 2 BotNet Documentation - Pastebin.com	Botnet & tools documentation, unchanged

6	s8bxn - Ghostbin	DDoS Guide & active target list, unchanged
6	propaganda-http///piratepad.net/5Fk0Ew0pNg	OpBashDaesh content for info-op, revised
6	z74o5 - Ghostbin	Twitter followers retriever, unchanged
7	[Python] TwitterReport (v.1.0.3) - Pastebin.com	Twitter reporter, unchanged
7	#opisis - Generation 2 BotNet Documentation - Pastebin.com	Botnet & tools documentation, unchanged
7	propaganda-http///piratepad.net/5Fk0Ew0pNg	OpBashDaesh content for info-op, unchanged
7	piratepad.net/bEJcSwtejH	OpBashDaesh info-op instructions
7	s8bxn - Ghostbin	DDoS Guide & active target list, unchanged
8	[Python] TwitterReport (v.1.0.3) - Pastebin.com	Twitter reporter, unchanged
8	#opisis - Generation 2 BotNet Documentation - Pastebin.com	Botnet & tools documentation, unchanged
8	Anonymous - Learn Arabic - FUCK ISIS - Pastebin.com	Arabic learning materials
8	Guide to Countermessaging _ #opBashDaesh	OpBashDaesh countermessaging instructions
8	propaganda-http///piratepad.net/5Fk0Ew0pNg	OpBashDaesh content for info-op, unchanged
8	s8bxn - Ghostbin	DDoS Guide & active target list, unchanged
8	z74o5 - Ghostbin	Twitter followers retriever, unchanged

8	Countermessages — For Westerners _ #opBashDaesH	OpBashDaesh countermessaging instructions
8	Countermessages – Daesh's Enemies _ #opBashDaesh	OpBashDaesh countermessaging instructions
8	CounterMessages_ For Potential Recruits _ #opBashDaesh	OpBashDaesh countermessaging instructions
8	More Countermessages _ #opBashDaesh	OpBashDaesh countermessaging instructions
8	Why'd he join ISIS_ Why'd you join Anonymous_ _ #opBashDaesh	OpBashDaesh countermessaging instructions

Table 14 Research materials indexed by model phase