CSS CYBER DEFENCE TREND ANALYSIS 1

Active Cyber Defense

Zürich, June 2017

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

CSS ETH Zurich

ETH zürich

Author: Dr. Robert S. Dewar

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zürich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group; Oliver Thränert, Head of Think Tank

Please cite as: Dewar, Robert S (2017). Active Cyber Defense, Cyber Defense Trend Analysis, Center for Security Studies (CSS), ETH Zürich.

Executive Summary

Objective

Cyber security is an important and highly topical security issue. It comprises a number of techniques and approaches to the securing of digital networks and infrastructures, as well as the systems which depend on them. Following several high profile incidents which occurred between 2007 and 2012, national and international actors are taking note of the importance of one particular aspect of cyber security: cyber defense.

As a result of the severity of these incidents, and allegations of state involvement, there has been an increased level of discussion at national policy level around how best to defend digital interests. Active cyber defense (ACD) is one mode adopted by a number of international actors. ACD is a concept predicated upon deploying tools to not only identify and stop cyber incidents as they are occurring, but also taking offensive measures to minimize attackers' capabilities. This can be achieved through a variety of technical solutions such as deploying decoys or hacking the attackers' own networks to neutralize their efforts. Despite the existence of these tools, ACD lacks conceptual definition.

This report has three goals. First, it seeks to add more clarity to ACD itself by defining the concept and contextualizing it alongside fortified and resilient modes of cyber defense. Although they employ distinct techniques these three approaches can best be employed together in a co-operative manner, a "triptych" of cyber defense. The second goal is to establish the prevalence of such measures in the strategies of important state and international actors. This is done in order to analyze whether there is a trend towards, or away from, active measures. Finally, the report provides some points of consideration when developing cyber defense policy. The most important of these are the need to conduct an effective cost-benefit analysis as well as ensuring a goal-oriented approach to selecting and deploying ACD tools.

Method

An analysis of current cyber security strategies was undertaken in order to assess the prominence of ACD as a policy choice. This allowed for the preference of ACD to be compared with other modes of defense and for the actors to be compared with one another, to see which was more "active" in their defense policy.

Eight states and two international organizations were selected for analysis. These ten entities were categorized according to their impact on international relations, whether they had been the victim of a cyber-attack or whether they had a comparable federal structure, such as Austria and Germany. A full methodological summary is included in Annex 1 of this report.

Results

The analysis found that ACD is not a widely deployed policy solution. Instead resilience is adopted as the policy of choice. Due to the extraterritorial nature of ACD there are legal and political ramifications to its use which reduce its desirability. Although several national actors and international organizations acknowledge the importance of identifying and neutralizing perpetrators of cyber incidents, there is a trend of applying ACD in concert with other, more resilience-oriented policy approaches. Where national policies include measures to promote prevention of incidents, rather than simply pursuing perpetrators or relying on the resilience of systems, a more holistic, strategic approach to cyber defense can be achieved. This can be held up as an example of best practice incorporating all three modes of cyber defense.

Disclaimer

It is important to note at this point that this report undertook an analysis of publically available national cyber security and defense policy. The report does not examine the tools used in the implementation of such public policies. This is an important distinction. Cyber defense and security policies are documents in the public domain. They are released to explain a government's position in the field, and provide some insights into how state apparatus intend to deal with cyber risks and incidents. The choice of tools adopted by a state as part of their cyber defense policy is often not made public knowledge. In certain cases, such as the UK and the US, cyber defense capabilities fall under the general remit of the security services. Tools used to achieve cyber defense therefore remain classified and were not available for analysis.

A second point of clarification is that the documents analyzed were all published in English. While this is of great methodological benefit (all policy documents can be analyzed in equal measure) certain allowances for translations and national cultural expressions must be acknowledged. An example of this is that Russian policy and publications do not use the term "cyber". Instead the term "information security" is used to refer to "cyber security".

1 Introduction

The number of breaches of information and communications networks, more commonly known as cyber-attacks, have increased exponentially in recent years. These network breaches range from direct assaults on government infrastructures to populist hacktivism and monetary theft. This trend has resulted in an increased social and political awareness of these incidents. Cyber defense is the use of digital tools to defend computer systems and networks from these cyber-attacks and malicious intrusions. Active cyber defense (ACD) is one way to achieve this. It is a particular technique distinguished from other approaches by having an offensive component. ACD tools actively seek out malicious intrusions and minimize their effects – either by destroying invading viruses or providing them with artificial, decoy data – and engaging with perpetrators of cyber incidents in some sort of active manner. The offensive nature of ACD tools can extend beyond the victim network. A technique known as hack-back (see Section 2.1.2 below) centers on defenders tracing the source of an attack, and neutralizing the perpetrators' own systems, effectively taking the fight to the enemy. US policy takes this proactive response to extremes, reserving the right to launch kinetic, i.e. physical, responses to cyber-attacks (USA, 2010, p. 14).

As a subject for academic study, ACD also increased in prominence since these incidents took place. The 2014 annual conference on cyber conflict hosted by NATO's Co-operative Cyber Defense Centre of Excellence (CCDCOE) was devoted purely to examining ACD from a technical, policy-oriented and legal perspective.

Despite this increase in political and academic prominence there is little agreement on what ACD actually is. It remains an often-discussed but ill-defined term. This lack of clarity is a hindrance both to the understanding of this concept and to the development of effective cyber security and defense policy. This report therefore proposes a definition of ACD which is useful for academic research and policy development. To support this definition, four prominent ACD tools are examined in this report: white worms; hack-back; address-hopping; and honey-pots. The purpose of this examination is not to recommend one particular technique over another, nor is it to present a comprehensive list of ACD tools. Instead the aim is to provide an introduction to the types of activities which constitute active cyber defense.

ACD is not a standalone policy option, however. It must be considered together with two other modes of cyber defense – fortification and resilience. Fortified Cyber Defense (FCD) refers to the practice of protecting assets behind digital perimeters such as firewalls. Digital fortifications are erected to prevent malicious intrusions into defenders' networks. Resilient Cyber Defense (RCD) is a pragmatic option focused on increasing awareness of cyber risks and anticipating threats. Doing so in an effective manner enables defenders to allocate resources more efficiently so as to ensure ongoing system functionality in the event of an incident. These three modes are not mutually exclusive. As presented in Section 3.3 they operate in a three-way relationship or "triptych" of cyber defense. This is important because effective cyber security and defense can be achieved only by employing aspects of all three approaches in a goal-oriented policy framework. Paying close attention to the objectives desired in a cyber defense policy or strategy will better inform the selection of cyber defense tools.

It is important at this point to clarify that ACD is not a function of "cyber warfare". Cyber warfare, or computer network operations (CNO), are offensive actions taken in the cyber domain during a military engagement or established conflict. Such operations can be pre-emptive or deployed in advance of a kinetic maneuver. ACD is a defensive technique. It is predicated upon identifying incidents, intrusions and perpetrators after an event. It is also not exclusively a military tool. Cyber defense techniques can be used by private corporations and other non-state actors without any state involvement. Any actor wishing to ensure the integrity of digital systems, whether they are a national agency or a private corporation, can engage in some form of active cyber defense. There are however, legal implications for such actions.

Cyber defense is therefore one part of larger strategic considerations for cyber security. It should be placed alongside CNO/cyber warfare concerns and non-ACD techniques. A strategic approach to cyber security incorporates all elements relating to data and human safety when interacting with the digital domain. That approach should acknowledge, however, that not all responses are appropriate all of the time. Certain tools and policy choices, such as CNO are only appropriate during times of conflict or war. Cyber defense techniques, including ACD, can be deployed during a conflict, but in certain circumstances can also be used during peacetime. They are therefore more versatile policy options than the development of purely offensive, military solutions to cyber security issues. Figure 1 below illustrates the relationship between the three policy approaches, showing how CNO/cyber warfare, ACD and non-ACD approaches sit under the larger heading of cyber security.

Scope of the Report

This introduction is followed by four chapters. Chapter 2 provides an overview and definition of ACD. Four techniques are examined in order to give an introduction to certain common methodologies. The chapter also examines the legal and resource implications of deploying ACD. Chapter 3 examines ACD in the context of fortified and resilient modes of cyber defense. It also explains

how they complement each other as part of a more holistic, strategic "triptych" of cyber defense. Chapter 4 sets out the results of the analysis of the 10 cyber security strategies. Chapter 5 concludes the report by presenting an examination of costs and benefits for deploying cyber defense measures as well as arguing in favor of holistic cyber defense policies. It also poses an important policy consideration: which national entities should be responsible for responding to cyber security incidents.

A detailed explanation and elaboration of the research techniques and methodology employed to conduct the analysis of cyber security and defense strategies is provided in Annex 1 at the end of the report.

Figure 1: Applicability of Cyber Defense approaches

<table>
<tr><td>Overarching policy</td><td colspan="3">CYBER DEFENSE</td></tr>
<tr><td rowspan="2">Situation in which Cyber Defense Technique is applied</td><td colspan="3">War/Conflict</td></tr>
<tr><td></td><td colspan="2">Peacetime</td></tr>
<tr><td>Cyber Defense Technique</td><td>CNO</td><td>ACD</td><td>Non-ACD</td></tr>
</table>

2 Active Cyber Defense: Conceptualization and Definition

The concept of active cyber defense lacks a clear formal definition (Giles and Hartmann, 2014, p. 23). It has been loosely described as the real-time capability to detect, analyze and mitigate threats (Rosenzweig, 2013, p. 2) or as "proactive measures launched to defend against malicious cyber activities or attacks" (Ducheine and van Haaster, 2014, p. 304). Other attempts at definition focus on actions taken to identify perpetrators and remove their capacity to either continue with an intrusion or conduct a future attack.

These descriptions share three important characteristics. First, there is an emphasis on the use of specific tools to counteract the immediate effects of a cyber-attack in victim networks. Second, there is a focus on developing capacities to engage directly with the perpetrators in their networks. The third characteristic is that there is some sort of interaction with an opponent, either directly or indirectly. As a result of the presence of these characteristics, ACD can be considered an approach to achieving cyber security predicated upon the deployment of measures to detect, analyze, identify and mitigate threats to and from communications systems and networks in real-time as well as the malicious actors involved. This requires that defenders have the capability and resources to take proactive or offensive action against threats as well as interact with malicious actors, both in the defended systems and in those malicious actors' home networks. The benefit of this conceptualization is that it covers both the capacity to engage in real-time identification of threats and perpetrators as well as engaging with malicious actors in their own networks.

2.1 Techniques and Tools of ACD

To better understand ACD, it is beneficial to examine certain techniques which fall under its banner. There are numerous techniques and technical measures which can be categorized as ACD. Four examples are described here: white worms; hack-back; address hopping and honeypots. These examples should not be considered an exhaustive list or the tools techniques and resources which can be considered as ACD, but a representative sample of some of the most common techniques available.

The defenders' intended goals are a crucial consideration when examining or selecting an ACD technique to deploy. Each of the ACD tools presented here fulfil different functions beyond the general, immediate act of defending systems and networks. Some techniques, including those selected for this report, become more or less relevant, suitable or appropriate given the relationship between the resources required to deploy an ACD technique, the ultimate goals of the defenders and the legal frameworks in which those defenders operate. Those goals and frameworks change depending on whether the defender is a private citizen, a commercial enterprise or a state security agency tasked with protecting national critical infrastructure. Any cost-benefit analysis undertaken when selecting or considering an ACD technique must make allowances for the ultimate aim of such actions.

2.1.1. White Worms

White worms (Lu et al., 2013) also known as "righteous malware" (Cobb and Lee, 2014, p. 71) are computer viruses deliberately deployed by a defender in their own network, usually with the knowledge of network users. Such viruses are labelled "white" to differentiate them from malicious, or "black" software (malware) which is deployed by attackers. White worms seek out such malicious intrusions. Once they are identified, the white worm can carry out a range of functions depending on its programming. Certain worms act like anti-virus software and destroy the intruder. Alternatively the intruder is analyzed to identify and locate perpetrators.

There are advantages and drawbacks to using white worms. An advantage is their persistent presence in defended systems and their constantly running, real-time analyses. Because they are always active, intrusions can be identified and neutralized before any damage occurs.

One drawback is that they are difficult to control once released into a network. This is particularly problematic if they contain self-replicating properties. As a system increases through the installation of additional devices or new software, the white worm replicates itself to ensure that all additions are protected. If a white worm escapes its home network, for instance through an internet connection or by transference on a USB memory stick, it will continue to replicate and carry out its functions. Although the initial intentions may have been to protect a network, once released a white worm can become a nuisance virus, or "black", simply due to uncontrollable replication.

A second drawback occurs if a white worm escapes or leaks from the defended network. Potential adversaries can analyze and reverse-engineer the worm's code, potentially enabling countermeasures to be developed and rendering the white worm useless. The discovery of Stuxnet in 2010 highlighted several of these risks. That virus was discovered and analyzed having been discovered in Belarus, after it had infected its intended target (Chen and Abu-Nimeh, 2011, p. 91).

In reality white worms are rarely used in an operational environment due to these drawbacks, and the inherent, substantial risks involved when deliberately introducing worms into a defended system, however well-intentioned that action may be. The cost implications

should a white worm "go rogue" are too high when set along-side any potential gains given that there is no guarantee that the white worm will identify attacks or intrusions.

2.1.2. Hack-Back

Hack-back is not a specific tool but a technique. It involves analyzing an intrusion to identify perpetrators and technology sources responsible for a cyber-attack and hacking them in return to neutralize their efforts (Curry, 2012, pp. 16–17; Heckman et al., 2013, p. 73). The attackers' own tools are being used against them but, crucially, this takes place in their systems and networks. This technique enables the neutralization of malware, the identification and prosecution of perpetrators and the impairment or destruction of malicious networks.

Hack-back can also be used to good effect while an incident is taking place. If a cyber-attack is identified and is ongoing, a defender can use hack-back techniques not just to take action against the opponent in real time, but also scan that opponent's network, examine how they interact with the defenders' systems and understand the target set of the attack. This information is useful not just for the complicated process of attribution, but also to identify potential future targets, or which defended assets are the most valuable and require the greatest attention on the part of the defender.

A significant drawback is the legality of such techniques. Using hack-back exposes the defender to the same legal sanctions as the attacker, especially where cyber-attacks originate extra-territorially (Deibert, 2009, p. 334). In this situation there are two issues of concern. The first relates to private sector engagement in ACD techniques such as hack-back. Large private sector corporations may carry out hack-back with the intention of responding to an act of corporate espionage in an attempt to regain control over proprietary information or recover trade secrets stored on a rival's network. To do so, however, would also constitute an illegal intrusion. The problematic nature of hack-back is increased exponentially if an analysis of an attack suggests state or state-sponsored perpetrators. Aggressive and damaging hack-back can have serious political or even military ramifications in such situations. Some actors, such as the US, state they are willing to use physical weapons as a response to a cyber-attack (USA, 2011, p. 14). The attribution of the intrusion must be accurate and reliable before such a response is initiated.

Due to the aggressive nature of hack-back and the potential legal ramifications of its use (even by legitimate state actors) special care must be taken when considering this tool. As with other ACD techniques, taking a goal-oriented approach in addition to a cost-benefit analysis can assist in the decision-making process. If a defender's goals are to identify and neutralize the servers from which a cyber incident is being directed while that incident is taking place, then hack-back can be a very useful and productive tool. If however, the defender's goal is to ensure ongoing system functionality and leave the cyber forensics until after that functionality is assured, then the potential costs of deploying hack-back tools begin to outweigh the potential gains. Other ACD techniques, such as honey-pots, can be utilized to examine the nature of a cyber incident – the code used, the assets targeted – and devise actions necessary to ensure functional continuity.

2.1.3. Address hopping

Address hopping is a defensive technique adapted from the practice of regularly changing radio frequencies in military field communications. In an ACD context, the sender's IP address is changed on a regular and quasi-random basis during the transmission of data (Shi et al., 2007, p. 295). This has the effect of requiring an attacker or eavesdropper to constantly search for and identify target data packets.

This technique has a number of advantages. An attacker must direct more resources to identifying data targets. This increases the probability of detecting intruders. Any traffic entering the defender's network, but addressed to non-existent or artificial addresses, would raise suspicion (Repik, 2008, p. 31).

Address hopping does contain certain logistical challenges, however. A sophisticated software and hardware infrastructure is required to establish and maintain effective hopping and monitoring of artificial IP addresses. Set-up costs for such infrastructures can be high in terms of financial and physical resources. For the defense of large-scale networks, such as national infrastructures, such costs require political decisions, both in terms of financial resources and in terms of which systems to prioritize.

2.1.4. Honeypots

Honeypots are decoys deliberately placed in a defender's network. These decoys simulate genuine software or data in order to provide artificial targets. Any activity undertaken on these decoys can be recorded, tracked and analyzed (Repik, 2008, p. 43). There are two types of honeypots (Spitzner, 2003, p. 62). "Research honeypots" analyze incidents to identify perpetrators and study attack methods and tools. As such they are labor- and resource-intensive for the defenders. "Production honeypots" identify malicious activity and generate alerts but conduct limited analyses for attribution. Consequently they are less resource-intensive to operate and maintain.

As a technique, honeypots have the advantage of being able to be deployed in a variety of network environments and situations and in both a preventative and reactive manner. Not only can they be deployed prior to an incident in order to protect genuine data and assets from infiltration or corruption, post-attack honeypots can be deployed once an incident has occurred. Such reactive honey-pots are useful once an incident has taken place and can be used to identify and analyze the malicious code away from genuine assets.

Honey-pots can also be particularly effective in wireless networks. Devices such as decoy broadcasters can be strategically placed in a Wi-Fi (W-LAN) area, such as a university campus or office. These devices inject artificial but realistic data targets into wider wireless traffic. The obvious drawback is ensuring that legitimate users of the wireless network can differentiate between genuine data and honeypot activity. Providing such details to legitimate users runs the risk of this data leaking out and being used by attackers to identify and avoid the decoys.

Another drawback is the potential legal fallout of deliberately providing artificial, simulated data in order to entrap would-be attackers. In certain legal jurisdictions, for instance the UK, such entrapment is outlawed and cannot be conducted by law enforcement authorities. As is the case with hack-back, care must be taken by defenders choosing to deploy honeypots as a solution, so that they are not exposed to legal sanctions.

An important final consideration with honey-pots is that they are resource-intensive. Designing, developing, deploying and maintaining honey-pots requires a great deal of time, expertise and expenditure, as well as careful on-going monitoring to ensure that they do not adversely affect the defended system. As such, a cost-benefit analysis must be undertaken prior to implementing this technique, with a particular focus on the goals the defenders wish to achieve. An ICT security company may wish to capture malicious intrusions or codes in order to examine and attribute them in a controlled environment. In this situation honey-pots can be effective tools. However, if an entity has a reduced focus or prioritization on forensic analyses and attribution of *malware*, such as a large financial services company, honeypots may be too costly given the ultimate goals of deploying ACD tools.

2.2 Limitations of ACD

In addition to the legal issues and ramifications surrounding offensive techniques such as hack-back, there are two further concerns which should be addressed before employing active measures: the effectiveness of ACD as a deterrent; and the resources required to conduct ACD activities.

ACD is problematic as a deterrent primarily because the techniques discussed above must remain secret to would-be attackers if they are to succeed. If it is widely known that honeypots and white worms are deployed in a defended network, attackers can spend time scoping that network to identify the defenses. This can then allow them to either reverse-engineer the defenders' software or develop targeted solutions to circumvent them. A well-known public example of this reverse engineering is the Symantec analysis carried out on the Stuxnet virus (Falliere et al., 2011). Although this example involved a software security firm decoding a malicious virus, Stuxnet was able to be analyzed only after its existence became public, negating its effectiveness as a tool. The same issue is a weakness of white worms or hack-back. ACD is therefore a technique with questionable effectiveness as a deterrent.

ACD techniques are also resource-intensive for the defender. White worms must be written and constantly updated in order to identify current and new intrusion types. Honeypots must be maintained and monitored to ensure no leaks or identification of artificial data. Hack-back requires human operators with hacking skills at least as effective as malicious actors. It also requires a speed of response not always available or practical in order to identify an attack, attribute it and conduct the hack-back with sufficient legal support. The installation and deployment of ACD tools as a policy option must therefore be carefully considered, and the costs involved weighed against the potential benefits. This cost-benefit analysis must also include the applicability of ACD techniques to any incident that occurs in relation to the objectives – the ultimate goals – of the defenders.

2.3 Application of ACD techniques

The four techniques outlined above are all classed as active techniques. They involve some sort of proactive effort to identify intrusions and take corrective action. However, not all techniques are relevant or suitable for all potential cyber incidents. Hack-back is not the most suitable response to a large-scale, widespread distributed denial of service (DDoS) attack such as that experienced by Estonia in 2007. The social and political priority is to ensure that the systems affected are restored and services return to normal as quickly as possible. Considerable resources are required to effectively conduct a hack-back, resources better allocated to restoring system functionality. Similarly, address-hopping would be a more suitable defense against website defacement than honeypots because the information on a website is publically known, but the IP addresses of servers hosting it are not.

Table 1 below lists certain types of hypothetical cyber-attack cross-referenced with ACD techniques. It illustrates which hypothetical situations may benefit from

certain ACD tools. The table is not exhaustive given the range of potential attack types, and the various tools and methods available under the heading of ACD.

Table 1 shows that no single ACD technique is applicable in every one of these situations. The use of ACD therefore requires not only a careful consideration of the potential costs involved, but also the applicability and relevance of the tool to the incident and the goals sought by the defenders. This question of relevance also has the potential to increase resources required to mount an effective active cyber defense if multiple techniques are required to defend different asset types.

Table 1: ACD tools and potential cyber threats

Legend: X = not suitable; √ = suitable

	White worm	Hack-back	Address hopping	Honeypot
DDoS attack (Estonia 2007)	X	X	X	X
Deliberate damage to targeted infrastructure (Stuxnet)	X	√	X	X
Corporate Espionage	√	√	√	√
Website defacement	X	X	√	X

3 Modes of Cyber Defense: Contextualizing active, fortified and resilient approaches to cyber defense

ACD is not the only option available to defend digital networks. This section of the report will briefly set out two further approaches to protecting digital assets: Fortified Cyber Defense and Resilient Cyber Defense. The section will contextualize ACD alongside these two modes and show how they are mutually complementary.

The delineation of fortified and resilient modes of defense occurred following a closer examination of non-ACD techniques (Dewar, 2014, p. 14). Such techniques were defined by Farwell and Rohozinski (2012, p. 109). 109) as "passive cyber defense". They included promoting good workplace practices such as secure passwords and encryption, partnerships between actors and agencies and greater situational awareness. However, the term was used as a catch-all to describe any form of cyber defense without an offensive component, including resilience and firewalls. This division is illustrated in Table 2 below. To further highlight this differentiation, the concept of computer network operations or CNO, the use of digital tools by the military in war-time, is also included.

Table 2: Division of tools by technique type

CNO	ACD	PASSIVE CYBER DEFENSE
Cyber weapons	Hack-back; Honeypots	All other non-offensive tools

This delineation is too simplistic, however. Just as ACD is not as simple as taking proactive action of any kind (some of which is classed as CNO), the installation of firewalls, information-sharing and the development of resilient networks which can cope with accidental or intentional damage are not simple, passive approaches. A closer examination of these techniques revealed that some were predicated upon setting up defensive perimeters – fortifications – and others focused on ensuring and maintaining system functionality – resilience. "Fortified cyber defense" and "resilient cyber defense" were therefore clearer, more nuanced definitions for non-active approaches.

3.1 Fortified Cyber Defense

In contrast to ACD, Fortified Cyber Defense (FCD) focusses on setting up defensive digital perimeters around key assets or potential targets (Dewar, 2014, p. 14). Techniques used to achieve this include firewalls and antivirus software. These are designed to minimize malicious access to defended networks. FCD is most effective when systemically secure communications and information networks and infrastructures are developed: security must be built into the system from the ground up (McGraw, 2013). This is because bolting off-the-shelf fortifications onto an existing network cannot adequately defend the whole system.

Because FCD is more effective when built into a system it can be resource-intensive. Decisions regarding the level of fortification required or necessary must be made at the commencement of a project or network construction. These decisions can increase set-up and construction costs. FCD can also be a low priority given the system being built. Until recently, guarding against a cyber-attack was not a high priority when building a hospital or a school. Other considerations were of more practical importance.

FCD also requires constant maintenance and updating. The nature of cyber risks and threats is constantly shifting, with new types of attack being developed and written all the time. This means that FCD defenses, such as firewalls, must be constantly updated to ensure they can withstand the latest attacks. Regular updates of the antivirus software or firewall on a home PC can achieve this, but the resources required to maintain this level of security increase exponentially when the system being protected is a large national or multinational network.

3.2 Resilience

Resilient cyber defense (RCD) focusses on ensuring critical infrastructures and services which rely on digital networks continue to function in the event of a cyber-attack. It takes two forms. Restorative resilience aims to return a victim system to a pre-incident status quo. This is also called "bounce back" (Herzog and Prior, 2013, p. 10). It reflects the ability of an entity "to respond, and recover, by returning it to a normal state of functioning" (Herzog and Prior, 2013, p. 10). In cyber defense terms, restorative resilience means halting a malicious intrusion and repairing its effects so that the system returns to the state it was in before the incident took place.

In contrast to bounce back, adaptive resilience aims to ensure that the victim system can change its status quo to reflect the new situation following an intrusion. The system alters its parameters to take account of the effects of an attack and continues to function. Given these two approaches, resilient cyber defense is there-

fore a strategic policy choice affecting an entire infrastructure rather than a specific technical solution or tool which can be installed at a key location.

RCD can be a more pragmatic approach than aggressively seeking perpetrators (ACD) or building defensive perimeters which require constant maintenance (FCD). This is because resilience anticipates that incidents will occur and focusses on preparedness and functional continuity. Resilient policies take account of risks unique to the system being protected, but also the general threat landscape. By maintaining this level of self-awareness, a resilient policy can respond to a cyber-attack on, for example, a power station by ensuring that electricity supply continues unaffected or, if affected, can be restored quickly and with limited adverse effects.

There are few dedicated techniques or tools for applying resilient policies. Unlike installing firewalls in FCD or conducting hack-back in ACD, resilience is a more abstract, strategic policy goal. It involves an examination of infrastructures to identify potential weaknesses and ensuring a systemic level of preparedness is in place should those weaknesses be exploited.

There are certain steps defenders can take, however, to improve system resilience and mitigate the impact of potential incidents. One of the simplest and most cost-effective methods is to take regular backups or copies of data and software so that systems can be restored in the event of an incident with minimal loss of data. However, a policy decision must be made as to the intervals between backups. Should an incident occur, any data created following the last backup could be lost. Defenders must make a decision as to what is considered an acceptable loss depending on circumstances. For a private home user, the loss of a month's worth of data will cause less long-term damage than for a large, multinational corporation. The corporation may instead opt for weekly or even daily backups, which is more resource-intensive. Additionally, simple software or data backups are only effective if the cyber incident does not target system hardware.

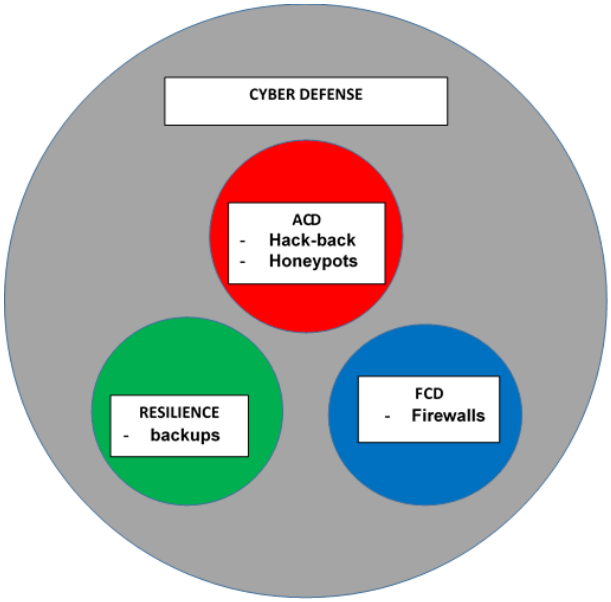
A second approach is the installation of redundant systems. This involves setting up a secondary network, kept completely separate from the main systems used. In the event of an incident affecting the primary network, the secondary system can be brought into operation. An advantage of the installation of redundant systems is that these can be initiated almost at the point of intrusion detection, with minimal loss of system functionality. However, this approach requires significantly more resources than simple backups, because a complete copy must be built, not just of data, but of the entire defended system, software and hardware included. This copy must also be kept separate to the primary network to avoid any malicious intrusions infecting it. Data from the primary system must also be copied at regular intervals onto the secondary network. This creates further potential opportunities to circumvent or breach network security measures.

Resilience in general provides a more anticipatory approach to cyber defense. By concentrating on system continuity and ongoing service functionality rather than prioritizing perpetrator identification, resilient policies provide a more strategic and preventive, rather than purely reactive, approach. However, a truly holistic cyber defense policy needs to incorporate all three modes of cyber defense.

3.3 The Triptych of Cyber Security

Cyber defense as a concept comprises three different approaches. There is fortification, where specific assets are protected by digital shields to prevent incidents or intrusions from occurring. Active approaches involve taking decisive action against a perpetrator, often in their own networks. Resilience focusses on system functionality, by ensuring a maximum level of preparedness. The policy choices are illustrated in Figure 2 below, within the wider context of "cyber defense".

Figure 2: The Modes of Cyber Defense



Although this conceptualization serves to highlight the differences in approach and technique between ACD, FCD and Resilience within the larger context of cyber defense, it oversimplifies the relationship between them. While each mode uses particular techniques, these techniques are most effective when deployed in concert with each other.

An advantage of resilient and fortified techniques is that they can provide certain protections unavailable to active tools. Table 3 below provides an update to the applicability of cyber defense techniques set out in Table 1. It shows which of the hypothetical cyber-attacks could have been prevented or mitigated by FCD or RCD, when ACD techniques were not appropriate.

Table 3 shows that where ACD measures would not provide a suitable mode of defense, such as a focused attack on an element of infrastructure or website defacement, FCD or RCD can. That is not to say that fortification and resilience should be employed instead of active measures, rather that they should be used together in a holistic approach. Resilience is a broad policy approach, and as such can incorporate elements of fortification to prevent breaches, but also ACD tools such as white worms to seek out malicious intrusions in order to reduce the length of time a system is affected.

The techniques and policy solutions of ACD, FCD and RCD therefore operate in concert with one another and often overlap in national policy approaches. Rather than form three separate approaches to defending digital systems, the three modes form a "triptych of cyber defense." A triptych is a set of three associated concepts which are best appreciated or considered together. In the case of cyber defense, ACD, RCD, and FCD have separate techniques, but are best viewed as three sections of a more strategic, holistic approach an updated version of Figure 2 shows the overlapping relationship between the three modes (Figure 3).

This mutually complementary nature is reflected in the fact that each mode can complement the others when deployed in the same system or policy. Assets are protected – fortified – by deploying measures such as firewalls to limit or reduce the chance of malicious intrusions being successful. Resilience enables systems to "bounce back" or adapt in the face of an incident and for functionality to continue should those fortification be breached. Once system functionality is achieved following an incident, ACD techniques can be deployed to identify, analyze and attribute the intrusion and enable the neutralization or impairment of the offenders' networks. This reduces the likelihood of future incidents taking place.

The overlap and complementarity of the three modes of defense is reflected in national cyber security and defense policies. The strategies of the UK and US include elements promoting active cyber defense. The US goes so far as to reserve the right to launch kinetic responses to cyber-attacks (USA, 2011, p. 14). Neither of these states are ignorant, however, of the need for critical national infrastructures to remain operational – be resilient – in the event of a major cyber incident.

Figure 3: The "Triptych" of Cyber Security

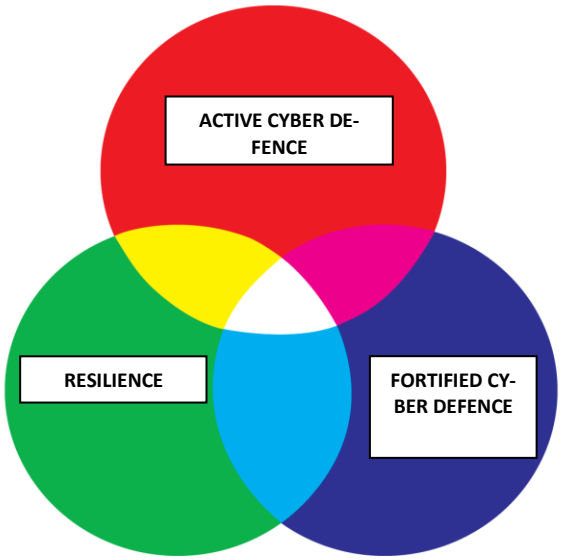


Table 3: Hypothetical cyber Incidents and modes of defense

Legend: X = not suitable; √ suitable

	White worm	Hack-back	Address hopping	Honeypot	FCD	RCD
DDoS attack (Estonia 2007)	X	X	X	X	√	√
Deliberate damage to targeted infrastructure (Stuxnet)	X	√	X	X	√	√
Corporate Espionage	√	√	√	√	√	X
Website defacement	X	X	√	X	√	√

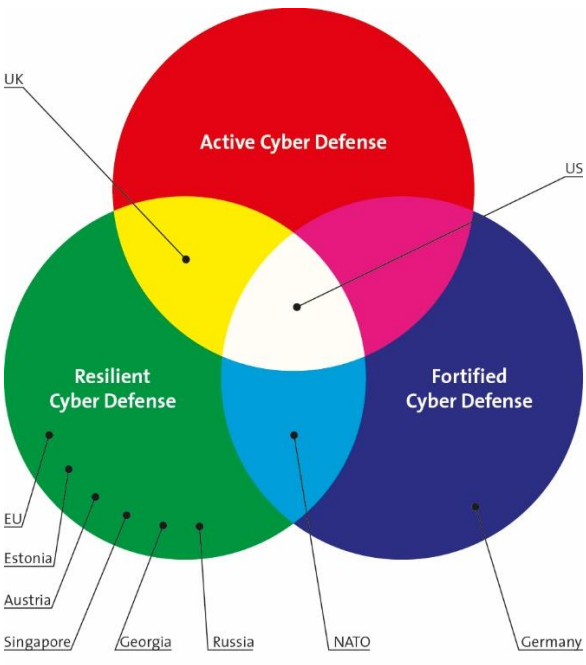
4 Analysis of Cyber Security and Defense Strategies

To determine whether or not there is a trend in policy towards ACD an analysis of national and international cyber security and cyber defense strategies was undertaken. A full, detailed methodology outlining the processes used to gather sources and analyze data is included in Annex 1. The report analyzed open-source, publically available government policies. Since 2010 the number of cyber security policy documents and strategies has increased exponentially. A representative sample of 10 entities (8 states and 2 international organizations) was distilled from this body of literature. These are:

- USA
- Russia
- UK
- Estonia
- Georgia
- Singapore
- Germany
- Austria
- The European Union (EU)
- NATO

To illustrate which actors favored which mode of cyber defense, they were mapped onto the triptych according to the occurrence of references to cyber defense. The results of this exercise are shown in Figure 4below:

Figure 4: Cyber Defense Policies by Country



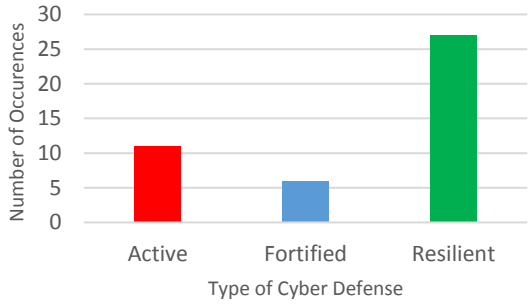
There are three main findings derived from the examination of these entities' cyber defense policies:

1. There is a trend towards resilience-based approaches to cyber defense;
2. This preference for resilience also extends to those states which have been the victim of a large-scale cyber-attack;
3. Only the USA occupies the "white zone", incorporating all three modes of defense.

4.1 Resilience as the preferred policy option

The analysis of national strategies supports the finding that there is a trend towards adopting resilience as a cyber-defense solution. Cyber defense was referenced 44 times in total. Of those 44 occurrences, active cyber defense appeared 11 times and fortified cyber defense appeared 6 times. Resilient approaches appeared 27 times, either as a primary policy option, or in concert with active and fortified modes. What the data analysis does not clarify, however, is whether or not there was a trend towards adaptive, "Bounce-back" resilience or restorative resilience. Statements from national policy advocating the resilience of systems range from prioritizing the importance of the ongoing functioning of the state and society (Estonia, 2008), restoration of compromised systems (Austria, 2013) to mitigating disruption to hardware (USA, 2011). This is summarized in Table 4 below:

Table 4: Occurrences of cyber defense type in policy



Resilience is a logical policy preference in today's wired world. A large number of control systems, communications networks and industrial infrastructures rely on the internet and an unimpeded data flow (European Commission, 2013). Due to this interconnectivity, the potential for a single network breach or incident in, for example, the banking sector cause a large-scale, nation-wide cascading failure is increased. The inherently transnational nature of online systems and internet communications means that this risk is raised to the regional and continental levels. State and regional policy priorities

are therefore focused on ensuring that the whole range of dependent systems continue running in the event of a malicious or man-made incident. That adaptive, bounce-back approach is crucial to the functionality and viability of state, regional and international systems. Resilience is, however, an unexpected preference in those states which have been the victims of cyber incidents with alleged state-sponsorship.

4.2 Victim States choose Resilience

The exercise of mapping the national actors on to the triptych also showed that while seven of the entities analyzed have single-policy approaches, none favored ACD. The majority of actors examined – 9 out of 10 – opted to include resilience, with 6 out of 10 opting for resilience as their sole policy option.

This was an unexpected result. Between 2007 and 2012 there was been a rise in the number and sophistication of disruptive incidents. The Estonian DDoS attacks of 2007, those in Georgia in 2008 and the Stuxnet worm fund in 2010 demonstrated a level of capability and sophistication of attack not seen publically before this time. Such an environment would logically lead to an increased securitization of cyber risks. Despite the increase in complexity and severity of network breaches, and the publicity and notoriety surrounding these incidents, the international community at the time demonstrated a considerable degree of pragmatism in its responses (Lonsdale, 2016, p. 54). This is shown in the preference for resilience over active modes of cyber defense.

This pragmatism is of particular note in the cases of Estonia and Georgia. Figure 4 illustrates that these actors also adopted resilient policies and so are positioned in the “green zone” of RCD. These states were among the first to be recognized as victims of state-sponsored cyber aggression or CNO. As such, a more active policy was expected.

There are two possible explanations for this restraint. One is the nature of the cyber-incidents carried out. This is particularly relevant in the cases of Estonia and Georgia. In the Estonian case the DDoS attacks experienced in summer 2007 were designed to impair social and financial systems in retaliation for the relocation of a Soviet war memorial (Gaycken, 2011, pp. 169–170). In Georgia in 2008 the aim was to spread anti-government propaganda and disrupt public service websites during the conflict with Russia in that year (Rid, 2013, p. 7). In both cases the targets were infrastructure systems which needed to continue functioning. As such, the immediate response on the part of both victims was to mitigate the effect of the attack rather than seeking to identify perpetrators and engaging in, for example, hack-back. The responses were restrained and pragmatic. Resources were better allocated to ensuring system continuity and functionality, hallmarks of resilient approaches to cyber defense. Only later were attribution processes undertaken.

A second possible explanation is the lack of international experience of cyber-attacks at the level of Estonia, Georgia and Stuxnet. While there is a history of computer network operations (Healey, 2013), only since 2007 has there been a publically known catalogue of major incidents with state involvement, both on the part of the perpetrator as well as the victim. Responding to such incidents with, for example, large scale kinetic force, would set an international precedent, one which would be difficult to roll back from and one which could lead to further escalation of conflict. Responding in the form of resilience means that states can be seen to be taking action, but in a far less politically sensitive manner.

5 Conclusions

There are three key points identified following the analysis of ACD as a concept and tool for cyber defense, as well as its propensity in national policy: the costs and potential benefits of deploying one or more cyber defense solutions; the overall benefit of a holistic approach to cyber defense and cyber security policy; and the need for a clear understanding of where responsibilities for cyber defense lie in state apparatus.

5.1 The need for comprehensive cost-benefit analyses before deployment of a cyber defense technique

One of the most important considerations for policy-makers when selecting a mode of cyber defense is the level of resources available and required to implement it, set alongside the potential returns in terms of system protection.

This report has highlighted a number of cost and resource considerations pertinent to the different modes of cyber defense. ACD techniques have the potential to be resource-intensive, particularly given the skill set and capabilities required to mount an effective hack-back, or the constant monitoring necessary when deploying white worms or honey-pots. Fortified solutions can be inexpensive if installed after a system has been set up. Certain software and hardware solutions can be bought "off-the-shelf" with generic security parameters pre-programmed (Deibert, 2009). Given the speed of technological development in cyberspace, retrospectively adding security measures is often the only option for system operators. However, the most effective solutions involve systemic security: networks where security solutions and measures have been built into those systems and networks from the ground up, often at their inception or at the design stage (McGraw, 2013). These can require substantial costs in set-up and design. Resilience requires a strategic, whole-of-system approach to cyber defense. Such a degree of self-awareness can require a considerable outlay of resources to ensure that as many infrastructure weaknesses as possible are identified so that contingencies can be developed. Such an approach requires decisions and choices to be made about the nature of the threats faced by the system, choices which could prove to be erroneous.

What needs to be considered when selecting a tool or particular type of defense is the potential return or benefit to be received from its deployment, i.e. how much protection is going to be ensured by the use of any given technique? Such consideration requires a comprehensive cost-benefit analysis to be carried out by policy makers, one which examines the defensive goals and levels of protection required.

5.2 Goal-oriented cyber defense

In addition to weighing up the potential gains from deploying an ACD technique with the potential risks and drawbacks of that technique, careful consideration must be given to precisely what outcome is sought from such deployment. A goal-oriented approach to active cyber defense, and cyber defense in general, can facilitate the selection of the most relevant and appropriate technique for a given circumstance as well as help in the cost-benefit analysis. The techniques examined in this Trend Analysis can achieve a number of objectives, from neutralizing a cyber-attack in real time or reverse-engineering that attack to identify the target set of an opponent, to potentially identifying the opponent themselves and taking offensive action in their network. As shown in section 2.3 above, not all techniques are appropriate in all circumstances. By ensuring that defenders are clear about their objectives, at both a general strategic level and the focused level of a specific incident, a more effective, holistic cyber defense can be achieved. Active cyber defense can therefore have a positive impact on wider cyber defense considerations when used appropriately.

5.3 The need for holistic cyber defense policies

No single technique or mode of cyber defense is suitable for all eventualities. Consequently, there is no magic bullet when selecting a policy approach. A holistic cyber defense strategy including all three modes of defense identified in this report can address a broad range of eventualities, while taking into account the costs and benefits of each mode, as well as the advantages and disadvantages of each technique relative to an actual or anticipated incident. It is also important to note that the costs of a large-scale cyber incident may not be purely material. A significant cyber incident can result in reputational damage if the defender has only taken minimal steps to guard against such intrusions. Equally, reputational damage can be suffered if the defender is perceived only to be interested in hunting down perpetrators without focusing on repairing any damage done or recovering any stolen assets.

From a technical and policy position the maximum level of defense against intrusions and incidents can be achieved by incorporating all three modes of cyber defense:

- Fortification means that assets are protected behind a secure system with limited or reduced chance of malicious intrusions;
- Building resilience into a system can help to maintain continued functionality, and allow

the system to "bounce back" or adapt if an incident occurs and fortifications are breached;
- Active cyber defense enables identification and analysis, and supports attribution of an intrusion. In certain circumstances it can enable the neutralization or impairment of the offenders' networks and thereby prevent or reduce the likelihood of future incidents taking place.

Adopting this policy position ensures the most holistic approach to cyber defense in peacetime. It provides for the greatest degree of protection with the widest range of possible approaches and techniques. As stated in Chapter 1, in 2016 the nature of cyber-attacks ranged from hacktivists breaching government websites to publish their message, criminal activity including data theft and suspected state-sponsored attacks on national infrastructures and systems. There have been numerous allegations that Russian specialists hacked the servers of the Democratic National Convention in the USA prior to the 2016 election (Rudnitsky et al., 2016), and the allegations and impact of their involvement in that election are currently being investigated. There is the threat of involvement or interference in the German and French elections of 2017. Resilient systems, ones that are able to continue functioning despite attempted or successful network breaches would minimize the impact of such activities. Resilience is therefore crucial to preventing the success of network breaches and mitigating the severity of network failures. But fortified (FCD) and active (ACD) cyber defense have their role to play as well. RCD mitigates the effects of all manner of network incidents, but FCD and ACD can counter or deter deliberate malicious acts. As the world becomes increasingly more wired, interconnected and communicative, the need for all-encompassing strategies employing a range of tools and techniques becomes clearer

5.4 Who is responsible for cyber defense?

An important corollary to this cost-benefit analysis and the development of a holistic policy approach is the question of who is responsible for launching, monitoring and maintaining a tool or technique. Much of the international digital infrastructure supporting cyberspace and the internet is privately owned. This raises the question of whether the private sector should shoulder the burden of responding to a large-scale cyber-attack or establishing defenses. There are several potential issues with such a situation. Assigning the private sector greater responsibility for securing an infrastructure of significant national importance has serious political implications. Consideration must be given to how far national governments are willing to cede national security responsibility to private entities. During this decision-making process consideration must also be given as to which resources to support – fortifications such as firewalls or resilience-based approaches. In states which operate on a federal structure, decisions also need to be made as to whether responsibility for the initiation and maintenance of cyber defense measures will held the national, regional or corporate level. Such a decision will also have resource implications. Local authorities may not have the technological resources to establish effective cyber defense solutions, while large, multinational private corporations have in-house security teams.

These considerations are complicated by the fact that any attempt to impose security requirements on private-sector ICT operators may face criticisms regarding internet regulation. In the wake of the release of classified documents by Edward Snowden in 2013 a number of data-gathering techniques used by state security bodies were made public. These tools were used, it was claimed, to ensure public safety. However, questions were raised over the extent to which national security agencies and apparatus had access to citizen data gathered by private ICT operators, and the manner in which that data was used (Hayden, 2014). If a policy decision is made in cyber defense which assigns greater security responsibility to private operators, the complicated relationship between government, security agencies and the private sector must be resolved or at least clarified. In other policy areas where a relationship between the public and private sectors exists, such as civil protection, the problem of which actor is responsible for security, and to what extent, is still being debated. The state can act as a facilitator or coordinator between public and private actors (Cavelty and Suter, 2009). In a policy area with a higher level of awareness for citizen rights and privacy, such as cyber defense, solution-building is even more problematic. More research is required in this area to identify the practices national, regional and municipal bodies use to resolve this issue. The trends identified in such an analysis would go some way to providing best-practice guidelines for assigning initiation and maintenance responsibility in cyber defense.

6 Annex 1 – Analysis methodology

The 10 entities examined in this trend analysis were selected based on five categories. The states were selected in order to provide examples in each category without overloading the analysis.

Category 1: Key State actors in cyber security

Actors prominent in international relations who also have a significant interest in cyber security and defense were placed in this category. It included the United States, the United Kingdom and Russia.

Category 2: Federal states

States with similar federal structures. Germany and Austria were selected.

Category 3: "Middle powers"

In international relations, middle powers are described as those which are "neither great nor small in terms of international power, capacity and influence, [but which] demonstrate a propensity to promote cohesion and stability in the world system" (Jordaan, 2003, p. 165). This is achieved through exercising soft power in international diplomacy (Bolton and Nash, 2010, p. 173). Due to its position as a financial and political center – an "issue specific power" (Neumann and Gstöhl, 2004, p. 5) – Singapore can be considered a middle power. Singapore was therefore added to the corpus for analysis.

Category 4: Victim States

These are states which have come under a large-scale, publically acknowledged cyber-attack. The most notable examples are Estonia and Georgia, which experienced distributed denial of service (DDoS) attacks in 2007 and 2008 respectively.

Category 5: International organizations (IOs)

This category comprised the EU and NATO. These entities were included to represent important IOs with a specific interest or strategy in cyber defense.

6.1 Conducting a metric conceptual content analysis

A challenge for this analysis was the absence of specific techniques in the majority of policy documents. The techniques discussed in Section Two of this report are not specifically cited in policy or strategy. Instead, ACD is inferred. In order to examine whether or not a policy or strategy is active in nature, these inferences were collated using a conceptual metric analysis. The strategy documents were therefore studied using a conceptual content analysis. This meant that the occurrences in those policies of *inferences* to active, fortified or resilient cyber defense were identified and catalogued, rather than specific words. Words and phrases which had conceptually similar meanings were identified and catalogued. This enabled the prominence of ACD as a concept, rather than a specifically defined or acknowledged practice, to be examined. A conceptual content analysis was required because the strategies do not mention specific techniques. Instead a mode of cyber defense is inferred by promoting, for example, measures to identify perpetrators and neutralize their capacities, an ACD approach.

The analysis of strategy documents was conducted using computer assisted qualitative data analysis software (CAQDAS), specifically MAXQDA. Once each document was uploaded into the software, they were analyzed and coded according to the preferred mode of cyber defense. This was achieved by conducting a conceptual metric content analysis. Words and phrases with conceptually similar meanings were catalogued, rather than numbers of words counted, as is the case in a standard content analysis. Conducting the analysis in this manner enabled inferences to particular modes, such as a promotion of resilience (RCD) or the need to develop measures to identify and neutralize malicious actors (ACD), to be counted and catalogued. It was necessary to conduct the analysis in this manner as there were no occurrences in the strategies of specific RCD, FCD or ACD tools.

7 Glossary of terms

Active Cyber Defense: an approach to achieving cyber security predicated upon the deployment of measures to detect, analyze, identify and mitigate threats to and from communications systems and networks in real-time as well as the malicious actors involved. This requires that defenders have the capability and resources to take proactive or offensive action against threats as well as interact with malicious actors, both in the defended systems and in those malicious actors' home networks.

Adaptive Resilience: a form of resilience where systems respond to an incident by changing operating procedures to account for any effects of an incident and so continue to function.

Distributed denial of service attack (DDoS): a type of cyber-attack where a targeted device, server or network is flooded with automated, artificial requests for access, thereby overloading and shutting down the system.

Fortified Cyber Defense: constructing systemically secure communications and information networks in order to establish defensive perimeters around key assets and minimize intentional or unintentional incidents or damage (Dewar, 2014, p. 15).

Resilient Cyber Defense: ensuring the continuity of system functionality and service provision by constructing communications and information networks with the systemic, inbuilt ability to withstand or adapt to intentional or unintentional incidents (Dewar, 2014, p. 15).

Restorative resilience: a form of resilience where systems respond to an incident by seeking to return to a pre-incident state.

White worm: a virus deliberately implanted in a system or network by that network's operator. Often designed to seek out and destroy malicious software. Contrast with Black worm, a virus inserted into a system to cause damage or steal data.

8 Bibliography

Austria, 2013. Austrian Cyber Security Strategy (National Strategy).

Bolton, M., Nash, T., 2010. The Role of Middle Power–NGO Coalitions in Global Policy: The Case of the Cluster Munitions Ban. Glob. Policy 1, 172–184.

Cavelty, M.D., Suter, M., 2009. Public-Private Partnerships are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection. SSRN ELibrary.

Chen, T.M., Abu-Nimeh, S., 2011. Lessons from stuxnet. Computer 44, 91–93.

Cobb, S., Lee, A., 2014. Malware is called malicious for a reason: The risks of weaponizing code, in: 6th International Conference on Cyber Conflict. NATO CCD COE Publications, pp. 71–84.

Curry, J., 2012. Active Defence. ITNOW 54, 26–27. doi:10.1093/itnow/bws103

Deibert, R.J., 2009. The geopolitics of internet control: Censorship, sovereignty, and cyberspace, in: Chadwick, A., Howard, P.N. (Eds.), Routledge Handbook of Internet Politics. Routledge, London, pp. 323–336.

Dewar, R., 2014. The "Triptych of Cyber Security": A Classification of Active Cyber Defence, in: Prangetto, P., Maybaum, M., Stinissen, J. (Eds.), 6th International Conference on Cyber Conflict. NATO CCD COE Publications, pp. 7–22.

Ducheine, P., van Haaster, J., 2014. Fighting Power, Targeting and Cyber Operations, in: Prangetto, P., Maybaum, M., Stinissen, J. (Eds.), 6th International Conference on Cyber Conflict. NATO CCD COE Publications, pp. 303–328.

Estonia, 2008. Cyber Security Strategy (National Strategy). Cyber Security Strategy Committee, Ministry of Defence, Tallinn, Estonia.

European Commission, 2013. JOIN (2013) 1 Final Joint Communication to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (Communication). European Commission.

Falliere, N., Murchu, L.O., Chien, E., 2011. W32. stuxnet dossier. White Pap. Symantec Corp Secur. Response 5, 6.

Farwell, J.P., Rohozinski, R., 2012. The New Reality of Cyber War. Survival 54, 107–120.

Gaycken, S., 2011. Cyberwar: Das Internet als Kriegsschauplatz. Open Source Press, Munich, Germany.

Giles, K., Hartmann, K., 2014. Socio-Political Effects of Active Cyber Defence Measures, in: Prangetto, P., Maybaum, M., Stinissen, J. (Eds.), 6th International Conference on Cyber Conflict. NATO CCD COE Publications, pp. 23–38.

Hayden, M., 2014. Beyond Snowden: An NSA Reality Check. World Aff. 176, 13–23.

Healey, J. (Ed.), 2013. A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Atlantic Council, CCSA.

Heckman, K.E., Walsh, M.J., Stech, F.J., O'Boyle, T.A., DiCato, S.R., Herber, A.F., 2013. Active Cyber Defense With Denial and Deception: A Cyber-Wargame Experiment. Comput. Secur.

Herzog, M., Prior, T., 2013. The Practical Application of Resilience: Resilience Manifestation and Expression. Eidgenössische Technische Hochschule (Zürich) Risk and Resilience Research Group Schweiz Bundesamt für Bevölkerungsschutz.

Jordaan, E., 2003. The concept of a middle power in international relations: distinguishing between emerging and traditional middle powers. Politikon 30, 165–181.

Lonsdale, D.J., 2016. Britain's Emerging Cyber-Strategy. RUSI J. 161, 52–62.

Lu, W., Xu, S., Yi, X., 2013. Optimizing Active Cyber Defense, in: Decision and Game Theory for Security. Springer, pp. 206–225.

McGraw, G., 2013. Cyber War is Inevitable (Unless We Build Security In). J. Strateg. Stud. 36, 109–119. doi:10.1080/01402390.2012.742013

Neumann, I.B., Gstöhl, S., 2004. Lilliputians in Gulliver's world. Small States Int. Relat. 3–38.

Repik, K.A., 2008. Defeating adversary network intelligence efforts with active cyber defense techniques. DTIC Document.

Rid, T., 2013. Cyber War Will Not Take Place. Hurst, London.

Rosenzweig, P., 2013. International Law and Private Actor Active Cyber Defensive Measures. Stanf. J. Int. Law 47.

Rudnitsky, J., Micklethwait, J., Riley, M., 2016. Putin says DNC hack was a public service, Russia didn't do it [WWW Document]. Bloomberg. URL http://www.bloomberg.com/politics/articles/2016-09-02/putin-says-dnc-hack-was-a-public-good-but-russia-didn-t-do-it (accessed 10.25.16).

Spitzner, L., 2003. Honeypots: tracking hackers. Addison-Wesley Reading.

USA, 2011. International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World (National Strategy). The White House.

USA, 2010. National Security Strategy (National Strategy).

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.