CSS CYBERDEFENSE TREND ANALYSIS 2

Cyberweapons: Capability, Intent and Context in Cyberdefense

Zürich, November 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; Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Andreas Wenger, Director of the CSS

Please cite as: Dewar, Robert S. (2017). Cyberweapons: Capability, Intent and Context in Cyberdefense, Cyberdefense Trend Analysis, Center for Security Studies (CSS), ETH Zürich.

Executive Summary 4

1 Introduction 5

2 What is a cyberweapon? Summary of the debate on definitions of cyberweapons 7
2.1 Classifying cybertools as cyberweapons 7

3 Timeline of incidents 10

4 Trends in cyberweapons use: 12
4.1 There are only three types of cyberweapon routinely deployed 12
4.2 There is a low number of incidents in which an actual weapon was used 14
4.3 Cyberweapons are deployed in already existing rivalries and conflicts 15

5 Conclusions and Recommendations 17

Glossary 18

Bibliography 19

Executive Summary

Objective

The number of cyberincidents occurring globally is increasing. These incidents range from hacktivist defacement of websites and theft of login details for users of online services to large-scale ransomware attacks and state-sponsored network intrusions. One of the most important aspects to be considered when devising policy solutions and responses to these incidents is understanding the tools that have been used to carry them out. Some of the most high profile cyberincidents of the last decade have involved the deployment of cyberweapons, a highly sophisticated set of tools specifically designed to cause harm or damage. The impact of these cyberweapons – ranging from digital to physical damage – has elevated them to the level of national policy discussions.

Conceptually, however, cyberweapons are inadequately and inconsistently defined. Legal definitions point to their being necessary for a cyberincident to be considered an armed attack under the Laws of Armed Conflict. More abstract examinations define cyberweapons very loosely as being digital instruments of harm, with little exposition of what that harm is. Such definitions also take little to no account of the context in which a cyberincident takes place, the intent of the perpetrator, or the dual- or multi-use nature of the tools used to carry out an incident. Cybertools can have benign applications behind their creation, but can be used as malware or weapons. This problem is summed up by the point that all cyberweapons are tools, but not all cybertools are weapons.

This conceptual fog creates a number of difficulties. It increases the challenges for policy-makers when seeking to develop appropriate responses to an incident, when deciding on the legitimacy or otherwise of a cybertool's use, or when seeking to develop cyberweapons norms in international law, such as arms control treaties.

This Trend Analysis (TA) has three goals. First, it proposes a method of conceptualizing cyberweapons which moves beyond technical, abstract or legal definitions. Instead it focusses on two specific conditions: the intent of the actor using the tool and the tool's impact. This proposal will make it easier for policy-makers to respond effectively to cyberincidents. Second, the TA provides an empirical grounding for this set of conditions by applying it to a series of well-known and documented cyberincidents. Third, the TA will explore three core trends identified in this empirical exercise.

Results

The empirical analysis of cyberincidents in which a cyberweapon was used identified three trends. First, despite significant advances, innovations and increases in complexity, there are only three actual weapon types: worms; botnets; and specifically designed weaponized code. These three types of cyberweapon are routinely deployed because they have been proven to be effective and because the fundamental structure of the internet, and world-wide web has not changed in the last ten years.

The second trend identified is that there are very few cyberincidents where an actual weapon was deployed. The vast majority of cyberincidents recorded in the public domain use other techniques (such as social engineering) to extract target data or were acts of vandalism such as website defacement. The aims of the perpetrators in these instances is not to cause damage, but is often criminal gain. Nevertheless, the incidents where a weapon *was* deployed have had a disproportionate impact on cybersecurity debate and policy development.

The third identified trend is that, when weapons *were* used, this use occurred in highly specific circumstances, such as the rivalry between Iran and the US, the conflict between Russia and Georgia and the Syrian civil war. The use of cyberweapons is therefore not only infrequent, but occurs within a very specific geo-political context: an existent conflict.

The results of this empirical exercise and reconceptualization of cyberweapons can help practitioners and policy-makers by providing an area on which to focus when devising responses to cyberincidents. Instead of trying to prevent *all* cyberincidents from occurring or having a negative impact on national or regional infrastructure, one possible approach is to devise responses which focus on the contexts in which cyberweapons are deployed and use these contexts to develop a resilience-based approach to cybersecurity and cyberdefence.

Disclaimer

The data for this Trend Analysis was drawn from available open-source material which is of great value but is also problematic. Many incidents, both in the private and public sector, go unreported due either to their classified targets or fear of reputational damage. The latter is particularly the case for multinational corporations not wanting to appear unable to adequately secure their assets or customer details. As a result, building a complete data set of international incidents is challenging. The incidents catalogued here are already in the public domain and are well documented in cybersecurity and defense literature. As a result, the data set to be presented here is representative, but nevertheless comprehensive enough to draw the conclusions presented in the Trend Analysis.

1 Introduction

Computers, networked devices and software have been used as tools for malicious activity since the mid-1980s. Since that time, the tools and techniques used in those malicious acts have increased in complexity and sophistication leading to the development of "cyberweapons" – digital tools capable of causing physical damage, destruction and disruption. As a result of a few high-profile cyberincidents such as the discovery of Stuxnet in 2010 cyberweapons are being discussed at the highest political and social levels, and in the same manner as weapons of mass destruction (WMDs).

The potential global impact of cyberweapons has been well documented in academic, media and policy literature (Dinstein, 2012; Kelsey, 2008). The impact is global both in the sense that a weapon can affect a single international network, or can affect multiple systems across the globe. News, policy and industry publications also frequently refer to cyberweapons in a variety of contexts from their potential use being classified as a war crime (Kelsey, 2008; Lin, 2017) to the constant threat of cyber war due to the equally constant threat of cyberweapons use (Daniel, 2017; Liff, 2012). Terms such as "cyber war" and "cyberweapon" make attention-grabbing headlines (Liff, 2012) which in turn can fuel or steer policy responses. This creates a climate of fear and hypersecuritisation (Hansen and Nissenbaum, 2009) of the cyber domain which may not be realistic and is certainly not helpful when developing policy at the national or international level. Nevertheless, the increased level of political discussion and the potential reach of a cyberweapon demonstrates that cyberweapons have "come of age" and are being considered as part of a state or international actor's strategic capability.

Despite this coming of age, the nature of cyberweapons – what they actually are – is still a subject of debate and discussion. Conceptualizations of cyberweapons range their being described as the defining feature of armed attacks under international law to more abstract definitions such as being instruments of harm. The problem with such definitions is that they focus on the nature of the device used in a cyberincident and take little account of context. This is particularly problematic given that a cybertool – for example a piece of self-replicating software – is not intrinsically a cyberweapon if the intent of the user is *not* to cause physical or digital damage. This generates complications for policy-makers because, while every cyberweapon is a tool, not every tool is a cyberweapon. This is an important distinction and makes effective classification of cyberweapons important, especially given the difference in resources available and necessary when responding to the use of a cybertool or a cyberweapon. Law enforcement and criminal justice resources are more likely to be deployed if an incident has been effected by a highly sophisticated cybertool. However, if a cyberweapon was found to be deployed then national security or military capabilities may be called upon. Effective classification of tools and cyberweapons can make such highly-charged political decisions easier. What is germane to the decision-making process when a cyberincident occurs, therefore, is an understanding of the intent of the user and the impact (actual or potential) of the tool involved.

This Trend Analysis proposes to move away from such restrictive categorizations towards one based around certain well-established categories for classifying weapons. The classification proposed here is based on two conditions which need to be satisfied before a cybertool can be called a weapon: that the intent of the user was to cause damage and not access systems for criminal gain, and that the impact or potential impact – the capability – of the tool was to cause damage. If both of these conditions are met then the tool used to effect the incident can be categorized as a weapon. The advantage of this conceptualization is that it takes greater account of the context in which the device was used. It recognizes that cybertools can be used for both malicious and benign purposes (intent) and acknowledges that the same tool can be either destructive or passive (impact).

If these conditions are applied to examinations of cyberincidents, only a few of those incidents can be said to have involved the use of a cyberweapon. An analysis undertaken to provide an empirical base for the use of cyberweapons showed that, between 1988 and 2015, only nine cyberincidents involved tools which satisfied both conditions for being classified as cyberweapons. This is a relatively low number when compared to the number of incidents recorded. The analysis also found that, where a cyberweapon *was* deployed, it was used in the context of a pre-existing conflict or state of actor opposition. The use of cyberweapons is therefore heavily contextualized. Not only does there need to be a clear intent on the part of the user to cause damage, but there must also be a reason for the actor to do so. That reason stems from a state of antagonism between one actor and their opponents. This context is particularly important in examinations of cybertools,

The analysis also showed that there are very few actual cyberweapons for actors to choose from. Of the series of incidents examined, only three weapon types were used – worms, botnets and specially designed "weaponized" software. This dearth of variety in weapon types, coupled with the context-dependent nature of their use resulting in only a few incidents where cyberweapons were deployed, can help policy-makers and practitioners devise more nuanced and informed responses to the occurrence of cyberincidents.

This Trend Analysis will proceed as follows. Section 2 will examine the current debate around when a cybertool constitutes a cyberweapon. It will show that current technical definitions take insufficient account of the context in which a cybertool is used. To remedy this situation, the section will posit two conditions – intent

of the user and the impact of the tool – which should be met before a tool can be classified as a weapon. Section 3 of the TA will examine nine cyberincidents which satisfy these two conditions in order to provide an empirical basis for the classification of a cyberweapon. Section 4 will examine the three core trends that can be identified from the empirical analysis – that there are only a few types of cyberweapon, that only a few cyberincidents occurred where a cyberweapon was used, and that those incidents occurred in a specific context of pre-existing conflict or rivalry. Section 5 of the TA presents some conclusions and recommendations of benefit to policy-makers and practitioners.

2 What is a cyberweapon? Summary of the debate on definitions of cyberweapons

The purpose of this section of the Trend Analysis is to examine the various ways in which cyberweapons have been defined, and to provide a metric for future classification of cybertools as weapons. In order to develop effective policy to tackle the threat of cyberweapons, policy-makers must be clear on what those weapons are. This is a particular problem as academic, legal, political and military sources define them in different ways. The Tallinn Manual – an important work of legal opinion – defines cyberweapons as

> 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 (Schmitt, 2013, pp. 141–142).

On the face of things this definition is logical and concise. It describes a tool with an inherent destructive or deadly capacity. The problem with the definition is that it applies descriptions of conventional weapons to tools used in the cyber domain, in particular their use in "attacks" as defined by the international laws relating to the declaration and conduct of war. Another definition is offered by Rid and McBurney. They take as their starting point a much simpler definition of weapons in general, describing them as "instruments of harm" (Rid and McBurney, 2012). Cyberweapons can also be instruments of harm, in the sense that they have the capacity to cause damage or destruction. The Stuxnet worm identified in 2010 caused damage by feeding corrupted data into the control systems of an Iranian nuclear enrichment facility. The Iranians allegedly retaliated in 2012 with the Shamoon campaign, which resulted in digital damage, i.e. the wiping of data and operating systems in computers owned by Saudi Aramco, an American-owned petroleum company.

Neither of these definitions is completely effective, however. Rid and McBurney's definition are oversimplify the problem as it takes no account of the intention of the user of the instrument. The Tallinn Manual accepts that a weapon is a weapon by virtue of its *intended* use, but takes no account of the complexities of cybertools and the inherent multi-use nature of those tools used in cyberspace operations. A malicious cyber tool, such as a virus or a weapon, is only rendered malicious by virtue of its impact and the intended use of the developer. Those same tools can have benign uses, a fact lost in the Tallinn Manual's militaristic definition. The problem can be summed up like so: all weapons are tools, but not all tools are weapons.

The subjectivity and context-dependence inherent in such descriptions causes particular difficulty when categorizing cybertools as weapons. Tools such as self-replicating software or coding that seeks out specific network weaknesses can be used for malicious purposes as instruments of destruction or for criminal gain, as was the case with the Sony hacks of 2011[1]. In this case, the attackers sought to extract customer identification and payment data. However, as mentioned above, such software is not always designed to be malicious. When deliberately used in a network by that network's administrators, self-replicating software can seek out and identify flaws, faults and systemic weaknesses in security processes or infrastructure. In this case, the intent of the user of the software is not to cause harm or damage, but to identify areas which need strengthening in order to prevent damage. This is a core function of "white-hat" hacking or penetration testing (Martin, 2017) and separates such usage from the deployment of weapons, a dual-use ambiguity inherent to cyberspace and cybertechnology given both military and civilian IT tools operate on commercial computing infrastructures (Lindsay, 2012, p. 41)[2].

What is important, therefore, is not the design of the tool or its destructive capacity, but the context in which it is used. As a result, a way to resolve this definitional dilemma in the cyberdomain is to step away from an examination or focus on devices and tools and instead look at more conceptual issues regarding the incidents where the tools used could conceivably be classified as weapons. Specifically, combining an examination of the intentions and motivations of the users of the tool with the tools impact or potential impact *in a specific incident* can be more effective than applying definitions more appropriate to conventional weapons. The next section of this Trend Analysis suggests a two-part test which can be applied to analyses of cyberincidents in order to judge whether the tool used was a cyberweapon.

2.1 Classifying cybertools as cyberweapons

Due to the difficulty in classifying cyberweapons from a political, academic or legal standpoint, a standardized test or set of conditions for determining if a tool used in a cyberincident is a weapon or not may be beneficial. A test is suggested here which focusses on the intent of the perpetrator involved and the impact of the tool deployed.

[1] In April 2011 details of 77m user accounts were stolen from Sony's PlayStation network.

[2] Examined further in Section 2.2 of this Trend Analysis

2.1.1 Intent

Intent refers to the motivations and aims of the perpetrator or user of a cybertool. Gauging the motives or ascertaining the aims of a malicious actor are challenging due to the problems of effectively attributing a cyberincident[3] but it is possible to make an educated, reasonable assumption if the cyberincident and the tool used to conduct it are analyzed.

If corporate data such as proprietary information or customers' private details are extracted from a company's servers, as was the case with the Sony hack of 2011, then it can reasonably be assumed that criminal gain was the ultimate goal[4]. If, however, a network is hacked and a government website defaced (as repeatedly occurred during the Syrian conflict) but no data was stolen, then hacktivism was the most likely goal or motivation. In such cases, damage to the network or physical damage to infrastructure was not the aim, and it is therefore not appropriate to label the tool used to effect the incident as a cyberweapon. Even in cases of suspected state espionage, where government defense networks are breached and classified files accessed or copied, such an incident would not elevate the tool to the level of a cyberweapon, despite the national security implications.

The condition which needs to be satisfied in order for a tool's intended use to allow it to be classified as a cyberweapon is that the perpetrator *intended to cause some sort of damage or harm*. That damage could be the deletion of files or feeding corrupted data into industrial control systems, or societal harm caused by the disruption of critical services. If no damage or harm was caused, either because the tool failed or the attack was thwarted, but the *intent* was to cause harm over and above personal gain, then the tool can reasonably be classified as a cyberweapon.

As stated above, the incident and tool employed in that incident must be examined in order to ascertain the perpetrator's motive, at least to a reasonable degree given the evidence available. This can be problematic because, as with accurate attribution, accurately determining a digital actor's motives can be difficult and labor-intensive. Nevertheless it is possible to make reasonable assumptions based on that evidence. If the intention of the perpetrator can reasonably be stated to be one of inflicting damage, then the tool can be classified as a weapon. If the intent was the profit or another sort of gain for the perpetrator, then the tool used remains just that, a cybertool. The main problem with this metric is the level of certainty with which it is claimed that damage was the intention. It is for these reasons that intent of the perpetrator alone cannot be used as a metric for determining whether a cybertools is a cyberweapon. Other criteria must be considered before a classification can be made, in particular the impact, or potential impact, of the tool and incident.

2.1.2 Impact

"Impact" refers to the destructive or deadly capacities of a cyberweapon. In this sense it relates to the so-called 'traditional' definition of a weapon as an instrument of harm. As discussed above, the nature of that impact can vary considerably, both in the aftermath of a cyberincident taking place, and in the medium to longer term. A cyberweapon such as Stuxnet had the effect of disabling a nuclear enrichment facility, but had the longer term effect of slowing down the Iranian nuclear program as a whole.

However, the nature of the impact must also be considered. Care must be taken when using impact as a metric to determine if a cyberweapon was deployed as that impact or harm need not be physical. While Stuxnet had a significant national security impact in that it ultimately caused damage to nuclear enrichment centrifuges. As a result, part of the fallout of the discovery of Stuxnet's deployment was a deterioration of political and diplomatic relations between Iran and the US and Israel, the alleged developers and deployers of Stuxnet. The point here is that similar impact can be achieved in a number of ways. Website defacement as a tool of cyberoperations is not normally classified as a weapon, but can have a significant destabilizing effect in the target area. If a government is seen to be unable to protect its national networks from such defacement, or if the effect of a hacktivist campaign is the weakening of citizen faith in their governing institutions, the impact of what is a relatively simple cyberattack can be significant.

Care must therefore be taken by decision-makers when using this metric. The nature and degree of damage – of harm – caused by cyber means varies depending on the incident. If death or destruction is the impact of a cybertool, then the tool can reasonably be described as causing harm. As a result of the varying types of cyberincident, the harm caused by a cybertool may not be physical destruction or the loss of data, but more abstract, social harm. This is the case when cybertechnology is used to disseminate (dis)information or propaganda against one or other party in a conflict, as seen in the Syrian civil war, or by publishing online images of dead soldiers (Conway, 2003). The harm caused in these socially focused incidents may well have an internally destabilizing effect on citizen morale and trust in government, but it is difficult to label these as weapons because the damage caused cannot be measured, nor was the intent to cause damage *per se*.

Not only can the impact of a tool be very different depending on circumstances – physical versus social

[3] An issue known as the "attribution problem"

[4] There are allegations of Chinese hackers stealing US military jet blueprints and building from them, but these are unsubstantiated beyond media outlets.

harm – but the same tool can be used to effect incidents of a different scale. Stuxnet is a type of malware known as a worm, but worms can be used to find particular data – such as computer files relating to a corporate competitor's unreleased products – to steal customer data as was the case in the Sony hacks of 2011. In both cases a worm was used to effect the incident, but the nature of the incidents were very different. The theft of customer or corporate data may have a significant impact and harm a corporation's stock price or consumer confidence, but may not have national security considerations.

As with an analysis of the intent behind the use of a cybertool, gauging the impact of the tool or incident cannot be used on its own when seeking to make decisions about whether a cyberweapon has been deployed or not. Combining such an impact analysis with an examination of the motivations or intentions of the actor behind the tool can provide a sounder empirical basis for a decision classifying a tool as a weapon. Such an empirical basis is very important and goes beyond the classification of tools as weapons given the range of response options available to a victim, particularly if the incident has a large-scale, national impact. If a state comes under a cyberattack the response options range from deploying national criminal justice resources – such as investigatory agencies – or national security resources such as the military or security forces. A political decision is necessary to ensure a suitable, effective and appropriate response to a cyberincident and a thorough examination of the intent and impact of the tool being used to effect that incident can inform that decision.

2.1.3 Two-Part test for determining whether a tool is a cyberweapon

Based on these two issues, a series of tests or conditions for determining if a tool deployed in a given incident was a cyberweapon can be developed by asking three specific questions. If the tool under examination satisfies these conditions, then the tool can be labelled a cyberweapon with a certain degree of confidence. These are:

1. What was the impact of the tool's use? Did it cause damage, destruction or death such as causing enrichment centrifuges to fail? If it did, then the tool used can be classified as a weapon.
2. What was the intent behind the tool's use? As examined in the section above, the same type of cybertools can be used to extract data for criminal gain, to cause a nuisance to the target or to cause damage. If the aim behind using the tool was to cause damage, then the tool can, in that incident, be classified as a weapon.

There are two caveats with this set of conditions which should be acknowledged at this juncture. First, the metric or series of conditions posited here is not intended to be a definitive test of the "weapon-ness" of a cybertool. Instead it is a proposal or suggestion for categorizing cybertools and weapons. The conditions set out here *can* be employed to provide a certain empirical base to such a decision. Ultimately, the labelling of a cybertool as a weapon is a political decision, given the nature or the incident and the range of responses available to a responding actor. The test provided here can provide a sounder basis for any decision which needs to be made.

The second issue relates to the speed of action required in the event of a cyberincident. Analyzing an incident, identifying actors and their tools and gauging the effects of those tools takes time. The speed at which worms and viruses can spread throughout a system and the speed at which infrastructures can fail due to that spread can dramatically reduce the amount of time available to analyze a tool and formulate an effective response to the incident. As with the labelling of a tool as a cyberweapon, the decision to respond to a cyberincident, and the nature of that response, is a political one and depends on available resources and capacities. However, investment in systemic resilience and infrastructures capable of "bouncing back" (Dewar, 2017) from an initial failure can buy victims and targets some time to effectively analyze the incident and formulate an informed and appropriate response[5].

[5] See Trend analysis 1

3 Timeline of incidents

With this set of conditions in place, it is possible to establish the nature of the cyberweapons to be examined in this Trend Analysis. The following section of the TA will examine incidents where the intention of the user of the tool was to cause damage, *and* where damage was caused, either physical or social in nature.

The proposed two-part metric outlined in Section 2 can be applied to historic cyberincidents in order to gauge whether or not a cyberweapon was used in those incidents. The object of this exercise is to provide an empirical basis for classifying cybertools as cyberweapons. It is important to bear in mind that the tools examined are not cyberweapons *in all circumstances*. The purpose of this empirical exercise, therefore, is not to state categorically which tools are weapons, but to demonstrate in which circumstances and contexts a cybertool can be classified as a cyberweapon in order that an informed political decision can be made about which resources to deploy in response to the incident.

Table 1: Cyberincidents where a cyberweapon was used

Year	Name of incident	Effect	Tool used	Weapon used? Yes/No	Intent of Perpetrator
1988	Morris Worm	Prank by US student caused 10% of fledgling Internet to fail	Worm	Yes	For worm to spread through digital systems without discovery. Replication of worm eventually causes device failure
2007	Estonia	Estonian government and banking websites and systems unavailable	DDoS through botnet	Yes	To prevent normal functioning of crtitical systems, and prevent use of social e-government and e-banking services
2008	Georgia	DDoS attacks on government websites as prelude to kinetic attack	DDoS through (suspected) botnet	Yes	Disruption of Georgian government networks and communication channels
2008	Conficker	Global effect: French navy computer network infected grounding aircraft; UK DoD systems affecting warships; German Bundeswehr; Computer systems of Manchester city council in UK	Worm	Yes	Disruption of critical military and police networked systems including aircroft control systems
2010	Stuxnet	Iranian nuclear centrifuges damaged	Worm	Yes	Cause damage to nuclear enrichment centrifuges and reduce neculear weapon production capacity
2011	Anonymous	Anonymous hacker collective hacks the Church of Scientology	Low Orbit Ion Cannon DDoS software	Yes	Hacktivist disruption of Scientologist websites to prevent access and use
2012 onwards	Syrian Conflict	Syrian Electronic Army (SEA) used software named BunderFucker 1.0 to target four international media outlets	DDoS with specially designed software	Yes	Alleged patriotic hackers promoting pro-Assad narratives and disrupting anti-Assad websites and news media outlets
2012	Shamoon	Iranian retaliation for Stuxnet: wiping of accessible and infected computers at Saudi Aramco	Timberworm worm for identification, network exploitation for access and Shamoon malware payload for wiping target machines	Yes	To spread worm through Aramco network which deletes and overwrites data on infected devices
2015	China	China uses its Great Cannon against US websites which listed other websites banned in China and which proposed sotfware to circumvent China's Great Firewall	Great Cannon DDoS software	Yes	To remove capacity for outside actors to influence its citizens

The empirical analysis exercise examined nine publically known cyberincidents between 1988 and 2015 which occurred in a range of international locations with a range of target types. It is also important to note that not all of the incidents were of a national security nature. Several were criminal acts, requiring a law-enforcement response. Nevertheless, the tool caused some sort of damage and the intent of the perpetrator was to cause that damage. The tool therefore satisfied the two conditions set out in section 1 above to be classified as a weapon. The results are set out in Table 1.

Table 1 shows that between 1988 and 2015, nine cyberincidents occurred in which a tool which can reasonably be labelled as a cyberweapon was used. The intent of the users ranged from disabling websites through DDoS attacks to grounding aircraft and causing physical damage to power grids or sensitive equipment. In each of these cases some sort of damage – physical or digital was the result, thereby satisfying both conditions for a tool to be classified as a cyberweapon.

The analysis exercise also provided an empirical base for three important trends. First, that there are only a few types of cyberweapon which are routinely deployed. Second, that there is a relatively low number of incidents in which a cyber weapon was used; and third, that when cyberweapons *are* used, it is within a recognizable geopolitical context, specifically an already existent rivalry or conflict.

4 Trends in cyberweapons use:

4.1 There are only three types of cyberweapon routinely deployed

The analytical exercise carried out for Section 3 demonstrated that there are three cybertools which are routinely deployed in a deliberately destructive capacity. These are:

- worms
- weaponized software and
- Botnets.

The first two types of cyberweapon are digital tools: malicious software known collectively as malware. The third type – botnets – differ from the others because a botnet is a hardware weapon comprising networks of infected devices. The following section of this Trend Analysis will examine each of these tools in turn, in order to provide more detail as to their purposes and functionality, as well as explain why, in certain circumstances, they can be classified as "weapons". While the list of examples used in the section is not exhaustive, it is sufficient to express the nature of the weapons and their targets.

4.1.1. Worms

Worms are pieces of malware which have the ability to replicate themselves and spread throughout a device or network. That replicability is programmed into the worm's coding. Worms can cause damage by targeting specific data sets on a network and deleting or corrupting them – as was the case with the Stuxnet worm and the Shamoon retaliatory campaign of 2012 against Saudi Aramco – or by compromising the integrity of data required for system functionality – as was the case with the original Morris worm of 1988. The most well-known and oft cited example of a worm is Stuxnet which affected the integrity of data being fed into enrichment centrifuges at Iranian nuclear facilities.

Another example is the BlackWorm, whose technical title is Win32/Mywife.E@mm (Microsoft, 2006) and was used by the Syrian Electronic Army (Baezner and Robin, 2017; Wilhoit and Haq, 2014). This worm uses a Trojan delivery system, in this case infected emails, to access target systems. The worm seeks out and modifies or deletes files and registry keys associated with certain computer security-related applications, thereby preventing these applications from running when Windows starts. This particular example describes a weapon targeting and affecting the integrity of data, rather than extracting or destroying information.

Worms can be classified as weapons because they have the capacity to cause damage such as deleting data. The destructive element of a virus is the unplanned or malicious removal of data from a system. Such data can also include core system functions on a CPU, e.g. Windows source code needed for the functioning of a device. Deleting such data renders the device inoperable (Miller, 2004). Data required for the operation of computer systems is not the only sort that can be destroyed. Proprietary data or digital records – such as bank accounts – can also be targeted and destroyed. Damage or destruction can also be caused by the worms compromising the integrity of data.

However, worms demonstrate the need for careful examination of the tools in order to determine if they are cyberweapons or not. This is because these malware demonstrate the inherent dual-use nature of certain cyber-tools. While worms can, in certain circumstances, cause significant intentional damage, in other cases their use can be benign. Worms can be used as "white hat" tools, for example by IT operatives in large corporations engaging in penetration testing. Such testing is carried out specifically to identify weaknesses, vulnerabilities and flaws in home networks, with the knowledge of the network owners. The intent behind the use of these malware in these instances is not to cause damage, but to identify ways to *prevent* damage. In such circumstances the use fails the first two of the three conditions outlined in Section 2 for classification as a cyberweapon: there was no negative impact, and the intention of the user was not to cause damage.

Not all cybertools have such clear, inherent dual-use features, however. Certain tools are specifically designed to cause intentional damage or harm, and are often created with a specific target in mind and it is to two of these tools, identified in Table 1, that this Trend Analysis will now turn: weaponized software and botnets.

4.1.2. "Weaponized software"

Weaponized software is a separate set of *malware* to viruses and worms. They are programs and pieces of software that have been specifically designed to cause damage to their intended target. They are not replicative: they do not move through a network or infect other machines as that was not their purpose. Instead they carried out pinpoint attacks on their target.

Two examples of weaponized software can be found in recent media and academic examinations. The first was nicknamed the Low Orbit Ion Cannon (LOIC). Developed by Praetox Technologies originally as a network stress-testing tool, its source code was made freely available on the Internet (Johnson, 2010). In 2011, the hacker collective anonymous deployed software specifically designed to effect DDoS attacks. Specialists at Anonymous developed a version which produced targeted DDoS attacks (Mansfield-Devine, 2011, p. 5) against, for example, the Church of Scientology (Norton, 2011). The attraction of this tool is that it can be used by low-skilled activists, i.e. those without a thorough or advanced level of computing

knowledge and is freely available online. While there are advanced options in the LOIC, certain of the core functions are available on a point-and-click basis.

The Chinese Great Cannon was also a piece of software specifically designed to create DDoS attacks on target websites. Rather than creating artificial requests, the action taken by the LOIC, the Great Cannon intercepts legitimate web traffic and reroutes it to its targets (Marczak et al., 2015).

The reason that this software can be classified as "weaponized" is because they are specifically designed to cause harm, damage or distress albeit originally under controlled conditions. The LOIC can be described as a tool "designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems or living things" (Rid and McBurney, 2012). Even under the definition proposed by the Tallinn Manual both of the LOIC passes the test of being weapons.

4.1.3. Botnets

Thus far the analysis has examined malware, programs designed for malicious purposes. These are all software. A cyberweapon need not be software, however, but can be a device or network of devices. Botnets are interconnected networks of infected devices – PCs, laptops or tablets – used to carry out network intrusions and breaches. The term "botnet" is an amalgam of robot and network. The description is derived from the fact that the legitimate operators of infected devices are often unaware that their device is being used for malicious purposes. Members of a botnet who are not aware of this membership are sometimes referred to as zombie devices.

At face value a botnet may appear to be a delivery vehicle, as infected devices are used to infect more devices and to carry out specific tasks, such as DDoS attacks. The 2007 DDoS incident in Estonia is widely believed to have been carried out by a Russian-backed botnet. However, despite being collections of hardware devices, botnets can be classified as weapons because they are used to effect an attack, causing damage by rendering target websites or servers inoperable. They can be considered the opposite of a kinetic cluster bomb. Instead of a single weapon damaging or causing harm to multiple targets, a collective digital weapon is used to focus on a specified target.

4.1.4. Why do these weapon types recur?

The identification of an empirically-based typology of cyberweapons begs the question: why do these weapon types recur in incidents where a cyberweapon was deployed? At a basic level, an answer to this problem is that there are only a few recognizable cyberweapons simply due to the problems of definition outlined in Section 1 of this Trend Analysis. Due to confusion surrounding what constitutes a weapon it is difficult to state when a weapon has been used in a particular incident. What is important is context and the classification of a tool under the intent-impact conditions categories: a tool used can be classified as a weapon if the intent was to cause damage, if the impact was achieved and damage caused. Because so few tools satisfy both of these conditions, there are necessarily very few weapon types.

This is only a partial answer to the question of this dearth of cyberweapon types, particularly given the large amount state and private resources which have been poured into cyberdefense and cyberoffense: why is it that these resources have been concentrated on developing tools within this narrow empirical typology? One answer is that these types continue to be effective. As shown in Table 1, the computer worm has been an effective malicious tool since the late 1980s. The 1988 Morris worm caused a section of the early internet to fail. Fast forward to 2010 and the Stuxnet worm fed corrupted data in SCADA systems leading to Iranian nuclear enrichment centrifuges spinning out of alignment and causing damage. Although the two worms were vastly different in terms of scale, target and technical sophistication, the fundamental premise – a piece of computer software able to replicate and search for targets independently of a human operator – remained the same. The continued effectiveness of these tools means that they are continually used.

Furthermore, not only are worms and viruses continually being used, but the same pieces of malware are also being recycled. In 2014 Sony Pictures was hacked, allegedly by North Korean pro-government agents (Gallagher, 2016). The tool used was a variant of the Shamoon worm used against Saudi Aramco in 2011. What makes these weapons attractive tools to use are the facts that such malware is freely available, has been shown to be successful and is relatively easy for someone with a certain, although limited, degree of technical capability to deploy. The hard work – designing and writing the original malware – has already been done. It simply needs to be customized, as was the case with Shamoon.

That being the case, if specific tools are needed for a specific purpose then these can be developed. As discussed in Section 3.2 the Low Orbit Ion Cannon (LOIC) is malware specifically designed to carry out DDoS attacks without the need for a botnet. In the Syrian conflict, the Bunder Fucker 1.0 malware was developed by pro-government actors to target and disrupt four international news media outlets (Baezner and Robin, 2017). There is also anecdotal evidence that, ironically, Bunder Fucker 1.0 was co-opted and used by rebel forces against pro-government media outlets (OpenNet Initiative and InfoWar Monitor, 2011).

These events show that such tools are effective and continue to be so. This ongoing success and effectiveness offers an explanation as to why there are only three types of cyberweapon identifiable in the

incidents currently in the public domain. The capacities and capabilities of these weapons has increased but the actual tool hasn't developed beyond a basic form because it has not needed to. This is similar to the development of nuclear weapons. Since the dropping of atom bombs on Hiroshima and Nagasaki in 1945, the complexity, sophistication and destructive capacity of nuclear weapons has increased, but the fundamental weapon design has remained largely static. A primary charge is used to ignite an uncontrolled chain reaction in nuclear fissile material. Such an increase in complexity around a static basic design is also the case in the development of cyberweapons. Since the release of the first publically identified worm in 1988, the complexity and functional capacity of this type of cyberweapon has increased exponentially, but its basic premise – malicious replicability inside a target system or network – has not changed.

Another explanation for the limited expansion of cyberweapons types can be found in the fact that the fundamental structure of the internet and its communications systems have also remained largely static in recent years. Malevolent actors are seeking to gain tactical or strategic advantage in a domain which has not seen major structural, functional or usage change since TCP/IP protocols and silicon computer microchips became the standard operating mechanisms. In the physical world there is a huge variety of kinetic weapons which are capable of having a multitude of effects, depending on the target and the operational environment in which they will be deployed. This is not the case for cyberweapons. They have only one operational environment, one which has not changed for some time. The amount of information communicated via the internet has increased exponentially, but the manner of that communication has not. Viruses and worms have become more sophisticated but their operational domain has not radically altered. The advent of quantum computing may cause such a shift, but it will be some years in the future before devices that use this technology have anywhere near the level of penetration necessary to require weapons to be specifically designed to operate in a quantum computer environment.

The exercise of cataloguing cyber incidents confirmed a number of well-documented trends. Cyber incidents occur around the world, affecting a variety of different state- and private-sector targets. Weaknesses in network security systems are frequently exploited (often zero-day vulnerabilities) by malicious actors searching for, finding and utilizing those weaknesses. There are, however, two core findings that warrant closer attention. First, there is a low number of incidents which can be said to have involved an actual cyberweapon. Second, of those incidents where state involvement is suspected, the cyber component of the incident did not occur in isolation. They occurred in the context of an existing rivalry or conflict. These two important trends will be examined in the following sections of this Trend Analysis.

4.2 There is a low number of incidents in which an actual weapon was used

The timeline of incidents providing empirical examples of cyberweapon use demonstrates that very few of the cyberincidents which occur utilize a cyberweapon. There were only nine instances recorded in the public domain between 1988 and 2015 in which a cyberweapon – a tool with both a destructive capacity and where the intent of the user was to cause damage – was used. One of those incidents – the Titan Rain campaign – is only *potentially* the result of the use of a cyberweapon[6]. This is a surprisingly low number compared with the 41 cyberincidents recorded between 16 and 31 December 2015 alone, according to the Hackmageddon public incident aggregator[7].

The reason for this low number is that few recorded incidents satisfy both conditions for being classified as cyberweapons. In the majority of incidents the intent – the goal of the malicious actor – was espionage or criminal gain, not damage. Analyses conducted by MELANI show that cybercrime – the theft of corporate data, hacktivism and espionage – are the primary intentions of malicious actors (MELANI, n.d.). These are criminal acts. The statistical preference for criminal action is supported by certain private sector analysts and incident aggregators such as such as Hackmageddon. According to that aggregators' reports, criminal activity routinely accounts for over 60% of recorded cyberincidents known in the public domain (Passeri, n.d.). This percentage occasionally reaches 80% (Passeri, 2017).

These statistics show that damage, destruction or death is not the primary intent behind the majority of incidents. The vast majority of cyber incidents involved the extraction of data for espionage or criminal purpose, or for propaganda purposes in the context of an existing rivalry. Despite the prevalence of cyber incidents, the number of times a cyberweapon was deployed is relatively low. The majority of cyber incidents catalogued utilized techniques (such as social engineering or exploiting system vulnerabilities) rather than actual digital or hardware *tools*. If, for example, an employee of a target entity can be manipulated into inadvertently divulging sensitive information through the use of phishing emails or other social engineering techniques, this is preferable to an attacker. Social engineering can potentially require more time to deploy but is less labor-intensive than identifying and exploiting

[6] While the effect and tool have been identified, there is insufficient open-source data to categorically state that the tool was a cyberweapon.

[7] Available at http://www.hackmageddon.com/2016/01/07/16-31-december-2015-cyber-attacks-timeline/

software vulnerabilities[8]. The majority of incidents therefore fail the first test for the tool used being classified as a weapon. Often the tool itself was not a digital device which would be weaponized. Techniques such as social engineering and phishing or the exploitation of unknown weaknesses in digital systems were the preferred tools.

The low number of incidents of weapon-use is significant for another reason: the disproportionate impact these few incidents have had on the wider cybersecurity debate. An incident on the scale of Stuxnet – in the sense that a cyberweapon ultimately caused physical damage – has not been repeated, but that incident is held up as the zenith of cyberwarfare capabilities and routinely cited in policy and research literature (Arquilla, 2013; Barzashka, 2013; Collins and McCombie, 2012; Herr, 2014; Schmitt, 2013). Similarly, the DDoS attacks in Estonia in 2007 were held up as the first example of a state-on-state cyberattack, given the allegations of Russian government-backing and support to the operators of the botnet used. Both these incidents are isolated in the context of malicious cyber activity, but have raised cybersecurity considerations to national policy, national security and military response levels.

This makes it even more important for policy-makers and scholars to examine the impact and intention behind incidents where cyberweapon use is suspected. The ramifications of a particular practical or policy response can be significant, and ripple far beyond the initial incident. If it is stated that the tool used in a cyberincident is a weapon, the incident becomes part of a small group of historical events, a club which includes Stuxnet, Shamoon and Estonia '07. This has the effect of raising its profile and significance, potentially beyond the level of attention it would have gathered had the tool not been declared a weapon. As a result of this heightened profile with potential national security implications, the range of potential responses becomes narrower with a concentration on the mobilization of national security or even military resources. Care must therefore be taken when describing cybertools as cyberweapons, even in a non-official capacity.

4.3 Cyberweapons are deployed in already existing rivalries and conflicts

The empirical examination of cyberincidents also identified that the majority of those cases where a cyberweapon was used occurred in the context of an already existing conflict or rivalry. "Rivalry" is a process of continuous conflict between two long-standing enemies (Bremer and Cusack 1995) characterized by repeated disputes. These disputes could be economic, involve political sanctions or all-out physical conflict. The criterion for a rivalry is that the two entities share some level of mutual animosity rather than a stable peace. The timeline in Section 2 shows that those cyber incidents occurred between states with a longstanding level of enmity – in short, classic rivals. The rivalry dyads identified were:

- The USA and Iran
- Russia and Estonia
- Russia and the USA[9]
- China and the USA

Where a state rivalry was *not* in existence, such as the hacker collective Anonymous targeting Scientologists or the release of the Conficker worm, a dyad exists consisting of two opposing sides, one seeking to influence or subvert the other by the use of cyberweapons. Although not a rivalry in the classic, state-centric sense of the term, the fact remains that there were two sides in the incident.

The occurrence of cyber incidents in situations of rivalry implies that such incidents do not occur in a vacuum: there is a defined and pre-existing context or scenario in which both sides are seeking tactical or strategic advantage over the other, or to adversely affect their opponent in some way. To achieve their goals, the parties use all available resources. In each of the four state-centric cases listed above, as well as in the case of the Anonymous DDoS attacks on the Church of Scientology, there as a history of antagonism which included political or economic sanctions, historical enmity or violence or an existent military conflict. In the case of Iran and the US, the US has been imposing sanctions, either unilaterally or through the international community, to reduce and restrict Iran's nuclear ambitions. In the case of the DDoS attacks on Estonia in 2007, the context was one of heightened political tension including the removal of a Soviet war memorial. Prior to the Russian attack on Georgia in 2008, the latter was subjected to a large-scale campaign of cyber-attacks, demonstrating how cyber capabilities complement kinetic action. The important point here is that a range of tools were being used. Rather than being the primary tool of choice, cyber capabilities were one part of an actor's complement or arsenal, to be drawn on when the need arose.

While this conclusion may not be unexpected, there are two points to make. First, it further reduces the prospect of a conflict in which cyber-attacks are the *only* feature. Secondly, if an incident occurs and there is *not* an existent conflict or rivalry, or the suspected originator of the incident is not one where there exists a longstanding feud or historical enmity, or if the target is not involved in any kind of wider regional instability,

[8] The small number of incidents in which a weapon is used is reduced even further if criminal activity is included. Criminal cyber incidents tend to also favour social engineering techniques to achieve goals.

[9] Although there is evidence to suggest the involvement of these states in the respective rivalries, there is only anecdotal evidence about their direct involvement in cyber operations against each other. This is due to the "attribution problem".

then the likelihood of the perpetrator seeking to cause damage by using a cyberweapon is reduced. Both of these points further emphasize the importance of examining and confirming context in the use of cyberweapons. Inter- and intra-state cyber incidents, operations and attacks may grab headlines and lead to policy or military responses, but they must be examined and analyzed in a wider geo-political context. In the case of the Russo-Georgian conflict, cyber-attacks were deployed as a prelude to Russia's conventional, kinetic operations and were designed to adversely affect Georgian communications systems. Understanding and being aware of this context can further aid policy-makers when making decisions on appropriate policy or resource responses to cyber incidents.

5 Conclusions and Recommendations

The goals of this series of Trend Analyses is to provide practitioners and researchers in the field of cyberdefense with ways to understand important issues in cyberdefense, and to enable the development of mechanisms to address those issues. This Trend Analysis has shown that the threat of cyberweapons is real and existent, by virtue of their having been used in a number of high-profile incidents. That threat, however, must be carefully considered and contextualized. The reality is that cyberweapons are a latent threat, but that threat must not be overemphasized. Such overemphasis can lead to knee-jerk reactions and heavy-handed or inappropriately severe responses. The key point to make is that cyberweapons are a rarity in studies of cybersecurity issues and catalogues of cyberincidents. Policy and resource management responses therefore need to be considered in a manner appropriate to this rarity.

Not only do deployments of cyberweapons rarely occur, but there are only a few types of weapon which are used. This means that those in a position to make decisions on which assets to defend and how to do so can examine the level of vulnerability and exposure present in their systems and take appropriate steps to minimize or mitigate the impact of the use of such weapons. By focusing on defending against types of weapons, potential victims in the private and public sector can better focus resources. There is a vast number of, for example, malicious worms in existence making it almost impossible to defend against each and every one specifically. However, defenders can ensure that their systems and networks can withstand worm intrusion by, for example, establishing system architectures and user procedures which minimize the potential for such malware to enter the defended system in the first place. It must be acknowledged that the use of specifically designed weaponized software (the second weapon type identified) is difficult to foresee and to guard against. However, if assets are adequately protected and made resilient, the potential *impact* of the use of such software can also be minimized. Good cyberhygiene can go some way to achieving these goals so raising awareness may be an effective solution to minimizing the effects of cyberweapons if they are deployed.

When cyberweapons *are* deployed, however, there are two important considerations policy- and decision-makers can keep in mind. The first consideration is whether or not a cyberweapon has actually been used, or some other type of cybertool. By examining the intent behind the tool, and the impact of its use, an informed decision can be made regarding the nature and level of resources – law enforcement or national security – which are used to mitigate or counter the incident. Second, the deployment of cyberweapons normally occurs within an already existent conflict or rivalry. That conflict could be an interstate or civil war, such as that between Russia and Georgia in 2008 or the continuing Syrian conflict. It could also be a clash of ideals such as that between Anonymous and the Church of Scientology. The point is that the use of cyberweapons does not occur in a vacuum: there is a reason for that use. By examining the context in which a cyberincident occurs, as well as the intent behind, and impact of, the use of cybertools, policy- and decision-makers will be in a better position to make more informed policy choices regarding appropriate responses and countermeasures. Such an analysis can also go some way to identifying the actors behind a cyberincident and therefore examine the tools used from an intent-impact perspective. Not only does this allow for a better understanding of the incident and potential responses, but it can avoid both overemphasizing the cyberincident and any potential escalation.

Glossary

Botnet or bot: Network of infected computers which can be accessed remotely and controlled centrally in order to launch coordinated attacks (Ghernaouti-Hélie, 2013, p. 427).

Hacktivism: use of hacking techniques for political or social activism (Ghernaouti-Hélie, 2013, p. 433).

Integrity of data: protecting data from modification or deletion by unauthorized parties, and ensuring that when authorized people make changes that shouldn't have been made the damage can be undone. Part of the CIA Triad of Confidentiality, Integrity and Availability of data. (Perrin, 2008)

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012, p. 81).

Phishing: technique used to trick a message recipient into giving confidential information like login credentials by thinking that the message came from a legitimate organization (Ghernaouti-Hélie, 2013, p. 437).

Social Engineering: a non-technical strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices (Lord, 2015)

Trojan (or Trojan horse): Malware hidden in a legitimate program in order to infect a system and hijack it (Ghernaouti-Hélie, 2013, p. 441)

Virus: Malicious program with the capacity to multiply itself and to impair the infected system. Its purpose is also to spread to other networks (Ghernaouti-Hélie, 2013, p. 442).

Weaponized software: programs and pieces of software that have been specifically designed to cause damage to their intended target.

Worm: Standalone, self-replicating program infecting and spreading to other computers through networks (Collins and McCombie, 2012, p. 81).

Bibliography

Arquilla, J., 2013. Twenty Years of Cyberwar. J. Mil. Ethics 12, 80–87.

Baezner, M., Robin, P., 2017. Hotspot Analysis: The Syrian cyber-battlefield.

Barzashka, I., 2013. Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme. RUSI J. 158, 48–56.

Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. doi:10.1080/18335330.2012.653198

Conway, M., 2003. Cybercortical Warfare: The Case of Hizbollah.org. Presented at the European Consortium for Political Research Joint Sessions of Workshops, Edinburgh, UK, p. 17.

Daniel, W. correspondent Z., 2017. Fancy Bear, Deep Panda and Charming Kitten: The faces of cyber warfare [WWW Document]. ABC News. URL http://www.abc.net.au/news/2017-07-16/crowdstrike-says-australia-vulnerable-to-cyber-attacks/8711312 (accessed 8.10.17).

Dewar, R.S., 2017. Trend Analysis 1: Active Cyber Defense.

Dinstein, Y., 2012. The Principle of Distinction and Cyber War in International Armed Conflicts. J. Confl. Secur. Law 17, 261–277. doi:10.1093/jcsl/krs015

Gallagher, S., 2016. Shamoon wiper malware returns with a vengeance [WWW Document]. Ars Tech. UK. URL https://arstechnica.co.uk/information-technology/2016/12/shamoon-wiper-malware-returns-with-a-vengeance/ (accessed 8.9.17).

Hansen, L., Nissenbaum, H., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. Int. Stud. Q. 53, 1155–1175. doi:10.1111/j.1468-2478.2009.00572.x

Herr, T., 2014. PrEP: A framework for malware & cyber weapons. J. Inf. Warf. 13.

Johnson, J., 2010. What Is LOIC? [WWW Document]. Gizmodo. URL http://gizmodo.com/5709630/what-is-loic (accessed 8.9.17).

Kelsey, J.T., 2008. Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare. Mich. Law Rev. 1427–1451.

Liff, A.P., 2012. Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War. J. Strateg. Stud. 35, 401–428. doi:10.1080/01402390.2012.663252

Lin, P., 2017. Why cyber attacks could be seen as war crimes [WWW Document]. Afr. Indep. URL https://www.africanindy.com/opinion/why-cyber-attacks-could-be-seen-as-war-crimes-10503493 (accessed 8.10.17).

Lord, N., 2015. What is Social Engineering? Defining and Avoiding Common Social Engineering Threats [WWW Document]. Digit. Guard. URL https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats (accessed 10.13.17).

Mansfield-Devine, S., 2011. Anonymous: serious threat or mere annoyance? Netw. Secur. 2011, 4–10. doi:10.1016/S1353-4858(11)70004-6

Marczak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott-Railton, J., Deibert, R.J., Paxson, V., 2015. China's Great Cannon [WWW Document]. Citiz. Lab. URL https://citizenlab.ca/2015/04/chinas-great-cannon/ (accessed 7.19.17).

MELANI, n.d. Situation Reports [WWW Document]. Report. Anal. Cent. Inf. Assur. MELANI. URL https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports.html

Microsoft, 2006. Malicious Software Encyclopedia: Win32/Mywife.E@mm [WWW Document]. URL https://web.archive.org/web/20060203115653/http://www.microsoft.com:80/security/encyclopedia/details.aspx?Name=Win32/Mywife.E@mm (accessed 4.26.17).

Miller, R., 2004. Symantec: New Virus Deletes All Files | Netcraft [WWW Document]. URL https://news.netcraft.com/archives/2004/06/08/symantec_new_virus_deletes_all_files.html (accessed 5.1.17).

Norton, Q., 2011. Anonymous 101 Part Deux: Morals Triumph Over Lulz [WWW Document]. WIRED. URL https://www.wired.com/2011/12/anonymous-101-part-deux/3/ (accessed 8.9.17).

OpenNet Initiative, InfoWar Monitor, 2011. Syrian Electronic Army: Disruptive Attacks and Hyped Targets [WWW Document]. OpenNet Initiat. URL https://opennet.net/syrian-electronic-army-disruptive-attacks-and-hyped-targets (accessed 2.14.17).

Passeri, P., 2017. Motivations Behind Attacks July 2017 [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2017/08/24/july-2017-cyber-attacks-statistics/ (accessed 8.28.17).

Passeri, P., n.d. HACKMAGEDDON [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/ (accessed 8.28.17).

Perrin, C., 2008. The CIA Triad [WWW Document]. IT Secur. URL http://www.techrepublic.com/blog/it-security/the-cia-triad/ (accessed 10.13.17).

Rid, T., McBurney, P., 2012. Cyber-Weapons. RUSI J. 157, 6–13.

Schmitt, M.N. (Ed.), 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare. CUP.

Wilhoit, K., Haq, T., 2014. Connecting the Dots: Syrian Malware Team Uses BlackWorm for Attacks [WWW Document]. FireEye. URL https://www.fireeye.com/blog/threat-research/2014/08/connecting-the-dots-syrian-malware-team-uses-blackworm-for-attacks.html (accessed 2.21.17).

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.