Cyber Warfare

Technical and Operational Aspects

Endre Wullum

Thesis submitted for the degree of
Master in Programming and Network
60 credits

Department of Informatics
Faculty of mathematics and natural sciences

UNIVERSITY OF OSLO

Spring 2020

Cyber Warfare

Technical and Operational Aspects

Endre Wullum

Cyber Warfare

http://www.duo.uio.no/

Printed: Reprosentralen, University of Oslo

Abstract

An increasingly interconnected world has given rise to a new digital arena for espionage, sabotage, and warfare. In this digital domain, nation-states are using cyber operations to wage cyber war on each other, where also private businesses and the civilian populace are increasingly caught in the crossfire. This thesis gives an overview of relevant literature describing multiple aspects of cyber warfare. It analyses to what degree cyber operations comply with national and international laws, and the limitations of those laws. It further shows that discrepancies are exploited by nation- states, and how this affects private businesses and the civilian populace. Finally the thesis evaluates some of the advanced ways in which organisations can attempt protect themselves from advanced nation-state threat actors, and conclude that this would be a daunting, if not impossible task for even the most powerful of organisations.

Acknowledgements

This thesis would not have been possible without a whole lot of people.

Firstly I would like to thank my family for all of the support, but also for allowing me to not talk about my thesis when visiting.

Secondly I would like to thank friends at Sofantos for helping to keep me sane throughout the production of this thesis. A special mention goes out to Ole Martin for some incredibly helpful and important advice on being a master's student, Daniel for always being willing to lend me an ear, as well as my roommate Christian.

Last, but not least, a massive thank you to my supervisor Audun Jøsang. Without his help, experience and patience this thesis would never have come about.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 It's All About Information Sharing

From its inception the Internet was about the sharing of information. ARPANET, the Internet's predecessor was established in 1969, and was developed to interconnect US universities with other governmental and military networks [18]. One of the core ideas behind the creation of ARPANET was to have a decentralized network of computers, so that the Soviet Union could not knock it out with a single attack. This decentralized nature is still at the core of the modern Internet.

With the creation of the World Wide Web (WWW), which is an application running on top of the Internet, during the years 1989 — 1991 the Internet became the universal fabric for interconnecting everything. The WWW turned the Internet into a truly open access platform that anyone could access from their home, and where anyone could participate. In recent years the Internet has continued to grow rapidly with the interconnection of IoT (Internet of Things) devices.

As the Internet has grown into an omnipresent cyber realm we have become increasingly reliant on it. The Internet is where we learn, work, pay our bills, and get entertainment. It has become an integral part of our everyday social life, and is always ready to be accessed through our smartphones. It is also a critical part of our society's critical infrastructure, with widely differing sectors such as banking, power grid management and supply chain management being very reliant on it.

But the Internet itself is still reliant on old communication protocols, some of which were developed in the days of the ARPANET. These protocols were developed in an age where access to networks were limited, and the actors who participated in the networks could trust each other. This trust was broken in 1998 when the first computer worm was created [71]. Almost 30 years after the creation of the ARPANET the Morris worm spread through the Internet, eventually taking down 10% of the servers and computers that were connected to the Internet [71]. The Morris worm was a wake-up call which prompted the investigation of security solutions to make the Internet resilient against malicious threats. We are still trying to build a secure Internet on top of these inherently insecure protocols.

1.2 Statement of the Problem

The increasing number of Internet-connected devices, combined with a growing reliance on the Internet for business, critical infrastructure, and social interaction means that the Internet has evolved into an increasingly prominent platform in every aspect of our society. It is also a shared platform used for governance, espionage, criminal activity, and even war. This has led to a paradoxical arms race where, on one side the criminals and nation-states are developing new methods to break into computer systems, while on the other side businesses and nation-states develop new methods to secure their computer systems.

How to securely navigate the cyber domain is becoming increasingly challenging. The best way of detecting, and thereby being able to mitigate, attacks come from openly sharing detection signatures in the aftermath of an attack. These signatures can be used to detect *indicators of compromise* (IOCs), e.g. artifacts left on the targeted system, or the tools, techniques etc. that are characteristic of an attack, a campaign of several similar attacks, or an attacker. These detection signatures stem from previous attacks and have to be continually developed and improved, or the detection capabilities will not keep pace with the development of new attacks.

Occasionally a new attack will be detected that has managed to avoid detection for weeks, maybe even months or years. Avoiding detection indicates a level of attack sophistication that is not common in most cyber attacks, as the attacks will have to avoid all forms of detection. Developing the tools to make such attacks can take months or years, and while detecting the attacks pose a challenge, the investment required by the attacker means they are unlikely to hit many targets. The tendency is that highly sophisticated attacks are also highly targeted, i.e. they will only target a few high-value targets.

This gives way to a problem affecting governments, national infrastructure and a select minority of businesses. How can they protect their computer systems from an attack that is not detected as it is happening? And is it possible to fully protect from an attack if the attacker is among the most capable cyber organisations in the world?

1.3 Research Questions

In discussing the problems outlined above, this thesis will give answer to some of these underlying questions.

1. In what ways are national and international laws enforced in cyberspace?
2. How does the relative lawlessness of the Internet impact people and businesses who are reliant on the Internet to perform daily tasks and do business?
3. How do nation-states exploit the relative lawlessness of cyberspace for cyber operations?

4. Assuming that an organisation has an extraordinary need for security, can it protect itself from the most resourceful threat agents in cyberspace?

1.4 Research Methods

The primary research methodology for this thesis is a systematic literature review, an analysis and comparison of how international law and regulations are applied to cyberspace versus the real world, and finally an evaluation of methods to protect against strong nation-state APTs.

1.4.1 Systematic Literature Review

Understanding of a field like cyber warfare must be achieved through a systematic literature review. Computer and network attacks are a considerable part of cyber warfare, therefore knowledge of these topics are essential to understand cyber warfare as a field. However, it is a complex field where multiple academic disciplines intersect, and as such, literature must be chosen from several fields of study. This literature sheds light on different aspects of cyber warfare, and so all disciplines must be understood in context of each other in order to see the full picture.

The first phase of this Master project focused on getting a general overview of what fields of study might be relevant when discussing cyber warfare. The main fields of study that have been included are information security, international law, especially the international laws and regulation that govern war, different national policies governing cyber operations, intelligence, corporate security, and modelling of threat scenarios.

Having identified what fields of study are relevant to the topic of this thesis, the next step was to identify areas of intersection between the distinct fields of study and cyber warfare. In identifying the information needed to shed light on the topic at hand some challenges became clear. In discussing operations, policies, strategies, and more that are by most countries considered sensitive, or even confidential, it is often challenging to find relevant documents and information.

1.4.2 Analysis and Comparison

An important part of the analysis was to look at how international laws and regulations apply to cyber warfare. War is, at least in the analog world, regulated by international treaties, e.g. the Hague and Geneva conventions. Other international agreements, such as the NATO treaty agreement does not regulate war, per se, but prescribe certain courses of action from members states, given certain circumstances.

After establishing how these laws, regulations, and agreements are enforced in the real world, the next task in this study was to investigate if they are transferable to the cyber domain, or if any cyber equivalent exists. The next part in the study was to compare implementation and enforcement in cyberspace to the real world.

1.4.3 Evaluate Methods to Protect Against Strong Nation-State APTs

The last part of the study was to identify possible security control that can be used to protect businesses from strong cyber attacks executed by nation-state actors. In addition these methods will include an evaluation of how well they can protect against the highly sophisticated nation-state APTs.

Chapter 2

Cyber Security and Cyber Operations

Information security can be understood as the preservation of *confidentiality*, *integrity* and *availability* (CIA). Confidentiality is maintained by preventing unauthorized disclosure of data, integrity is maintained by preventing unauthorized modification or destruction of data, and availability is maintained by ensuring that resources are accessible and usable on demand by authorized entities. Cyber security can then be understood as information security, as it applies to devices in or connected to the cyber domain.

In addition to the CIA triad, ensuring *authenticity* and *accountability* is also important to maintain information security. Authenticity ensures entity authentication and data origin authentication, i.e. that the identity of an entity is as it claims to be, and that the source of the data is as claimed. Accountability ensure that the actions of an entity can be traced uniquely to that entity, in order to support non-repudiation and traceability.

While there are many forms of computer attacks, at a high level they can be generalised to how they break the three components of the CIA-triad. Attacks such as these are illegal in most countries and are colloquially called hacking. However, when performed by someone sufficiently competent and resourceful, typically a nation-state, it is instead called cyber operations.

2.1 Cyber Operations

According to U.S. Cyber Operations Policy [48], *cyber operations* is the collective name for *cyber collection*, *defensive cyber effects operations* and *offensive cyber effects operations*. Definitions of these terms are summarized below. This document also provide definitions other than those covered by the term *cyber operations*. This includes network defense, an important part of cybersecurity, and cyber effects which is important in order to understand many of the other definitions.

These definitions have been created for use in the U.S. government and are defined by how they relate to U.S. law. They can, however, be

Level	Victim Posture	Characteristic Actions
0	Unaware	None: Passive reliance on inherent software capabilities
1	Involved	Uses and maintains antivirus software and personal firewalls
2	Interactive	Modifies software and hardware in response to detected threats
3	Cooperative	Implements joint tracebacks with other affected parties
4	Noncooperative (active response)	Implements invasive traceback, cease-and-desist measures, and retaliatory counterstrikes

Table 2.1: Levels of Intrusion Response [15].

generalised so as to apply to any country. While not all countries have laws similar to U.S. laws governing the cyber domain, all countries have a national interest in maintaining access to the Internet, and in securing their national infrastructure.

The U.S. Presidential policy directive/PPD-20 defines malicious cyber activity as activities that is not "authorized by or in accordance with U.S. law, that seeks to compromise or impair the confidentiality, integrity, or availability of [computer systems]" [48]. However, in this thesis malicious cyber activity will be defined by how it relates to national interests, rather than strictly how it adheres to U.S. law.

Network defense. Network defense is not considered a cyber operation, although it is essential in order to protect computer systems from intruders. Network defense is defined as the programs, activities, and use of tools conducted on a computer system in order to protect it, the data stored on it, or physical systems they control. These actions are conducted by, or with authorization by, the owner of the computer system.

According to the levels of intrusion response given in [15] (see Table 2.1), this definition of network defense would operate primarily at level 2. At this level the defender will actively change their software and hardware in response to threats, e.g. by blocking IP-addresses involved in an attack. It can also involve tracing the IP-addresses used by the attackers and reporting the attacks to the owners of the IP or law enforcement.

Cyber effects. Cyber effects are the results from certain cyber operations or cyber activity, such as "manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon" [48].

Cyber collection. Cyber collection is defined as covert operations and activities conducted, in or through cyberspace, for the primary purpose of collecting intelligence and information that can be used for future operations. Performed without the prior consent or knowledge of the owner or operator of the target system. Cyber collection includes activities enabling cyber collection, such as inhibiting detection or attribution, even if such activities create cyber effects. This can be considered the same as cyber espionage.

Defensive Cyber Effects Operations (DCEO). DCEO are defined as operations and activities, excluding network defense or cyber collection, conducted by or on behalf of the government, in or through cyberspace, in order to protect against imminent threats or ongoing attacks. These operations and activities can be performed by enabling or producing cyber effects outside government networks, without the prior consent or authorization of the owner of the computer systems. Such operations would be at level 4 in Table 2.1.

Nonintrusive defensive countermeasures (NDCM) are a subset of DCEO. NDCM are operations and activities that are performed with the prior consent or authorization of the owner of the computer system, and creates the minimum cyber effects needed to mitigate an attack. This implies that DCEO can produce more than the minimum cyber effects needed to mitigate an attack, e.g. pro-active defense or, if taken to the extreme, destruction of computer systems used to launch an attack.

Offensive Cyber Effects Operations (OCEO). OCEO are defined as operations and activities, other than network defense, cyber collection and DCEO, conducted by or on behalf of the government, in or through cyberspace, in order to enable or produce cyber effects outside government networks. Examples of such offensive operations could be Stuxnet [46] or the 2015 Ukraine power grid cyber attack [19].

2.1.1 Practical Limits of a DCEO

Flowers and Zeadally [21] argue that DCEO can be considered the same as active cyber defense. They created Figure 2.1, which illustrate how different incident responses fit into a spectrum from passive to active. In this spectrum the passive measures are more benign, while the active measures are more aggressive. This spectrum is roughly equivalent to Table 2.1 by Dittrich and Himma.

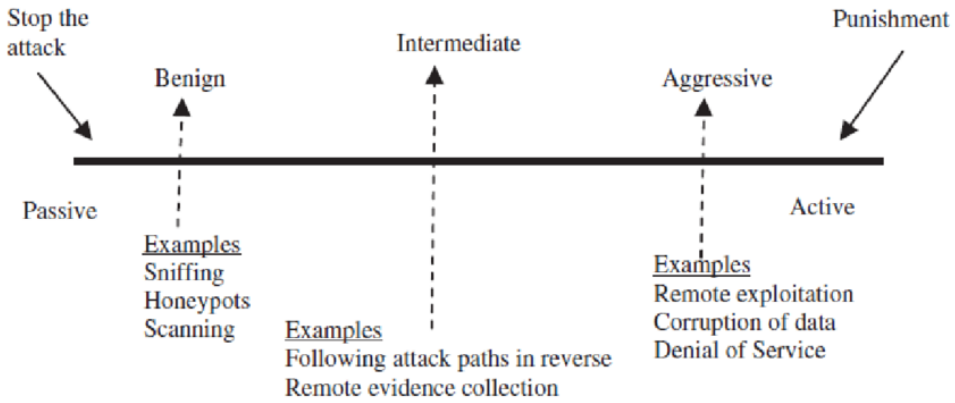

Figure 2.1: Cyber defense purpose spectrum [21].

At the more aggressive side of the spectrum in Figure 2.1, and corresponding to level 4 in Table 2.1 is where DCEO fits in. Dittrich

and Himma calls this non-cooperative measures [15], because they are carried out unilaterally by the defender. Such measures, they argue, can take several forms. They can be in the form of *cease-and-desist measures*, *retributive measures* or *preemptive response*. Cease-and-desist measures can be attempts to disable the attacker's computer system by exploiting common vulnerabilities. In the form of retributive measures DCEO could be performed by redirecting a denial of service-attack back at the attacker. While cease-and-desist measures aim to simply end the attack, retributive measures are intended to simultaneously punish and deter the attacker, in addition to ending the attack.

The last form of non-cooperative intrusion response, the preemptive response, pose "a host practical difficulties" [15], such as the cost to deploy and maintain the intelligence capabilities required to successfully detect and identify attacks before they are carried out, as well as the social costs of a public that might perceive a decrease in their personal privacy. Identification of an attacker, so-called *attribution*, is difficult, as will be discussed below in Section 3.1.3. Furthermore, misattribution can cause a lot of issues in the context of a DCEO, where an attacker can hop across networks in order to hide their tracks. This makes it difficult to determine if the target of the DCEO is the same entity that launched the initial attack difficult. Increasingly aggressive forms of DCEOs amplify these issues, therefore the defensive measures deployed must always be limited by the confidence of the attribution.

2.2 Cyberspace as a Domain of War

Cyberwarfare can be defined simply as warfare conducted in cyberspace, this definition is strengthened by the fact that several countries have already defined cyberspace as a domain of war. In 2011 the U.S. Department of Defence officially declared cyberspace as the fifth domain of war, alongside land, sea, air and space [14]. Five years later the members of NATO pledged to defend themselves in "cyberspace as in the air, on land and at sea" [47].

Cyberwarfare can, however, be a complex subject. Conventional warfare is governed by internationally recognized treaties and conventions. The declaration of war in particular is governed by the Hague Convention of 1907 [66], however these conventions do not seem to have carried over into the cyber domain. No nation has ever, overtly or publicly, declared a cyberwar against another nation.

There have been efforts to bridge this gap between cyber and conventional domains. The most exhaustive effort was initiated by the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCDCOE), which gathered a group of experts in international law to examine the law, as it exists, governing cyberwarfare. This became the Tallinn Manual [59]. This first version of the Tallinn Manual focused on cyber operations involving the use of force, and cyber operations used in support of conventional armed conflicts. A subsequent revised version has a broader focus, and

looks into cyber operations as they are performed, even in peacetime [60].

Cyber attacks such as Stuxnet [46] are generally considered to be an act of cyberwarfare. However analyzing such operations are challenging, and the definition of cyberwarfare is particularly tricky since the attacks happen without any formal declaration of war. The group of experts behind the Tallinn Manual tried to reach a consensus on whether or not the Stuxnet attack met the criterion to be characterised as an armed conflict, as they are defined in the Geneva Conventions I-IV article 2 [68]. They were unable to reach such a consensus [59]. One of the reasons making this characterization so difficult is that it is still not officially known if the attack were perpetrated by a state or by individuals, in fact no country or other actor have thus far officially accepted responsibility for the Stuxnet attack. The reasons for why it is so hard to determine who perpetrated an attack will be further discussed below in Section 3.1.3.

Despite NATO CCDCOE taking the initiative to create the Tallinn Manual, the Tallinn Manual is not an official NATO document, nor is it legally binding. In the introduction for the Tallinn Manual 2.0 [60] Schmitt makes it clear that the manual does not represent the views of the NATO CCDCOE, its sponsoring nations, NATO itself, nor any other state or organization. Specifically, the "*Tallinn Manual 2.0* is intended as an objective restatement of the *lex lata*[1]", as such the Tallinn Manual is an important step, but can not completely bridge the gap between cyber and the conventional domains, as it pertains to the international laws that regulate war. Successfully bridging this gap will likely not happen until the creation of an internationally accepted convention on cyber operations, analogous to the Hague and Geneva conventions.

2.2.1 Cyber Weapons on the Loose

One of the key rules of war is regulating how acts of war can affect civilians and civilian infrastructure. This has proved problematic on multiple occasions related to cyber weapons and their use in OCEO, as they can cause harm to civilians and third parties that are not specifically targeted, but also because the weapons have leaked, making them available for anyone to use. It is a well known fact that once something has been released onto the Internet, it is impossible to remove it.

The Stuxnet-attack was discovered in 2010. Because it was developed to spread easily via USB-devices, it started infecting third-party systems, rather than simply remaining on the targeted systems in the Natanz enrichment plant. When Symantec analysed the weapon they found that it had infected computers around the world, even in the USA [74]. Even though Stuxnet was highly targeted and unlikely to cause much damage to these third-party systems, the automated nature of proliferation meant that Stuxnet spread onto innocent computer systems, eventually infecting more than 100 000 systems outside of the target system.

The WannaCry outbreak in May of 2017 highlights another problem in

[1] The law as it exists

cyber operations. WannaCry was built on exploits leaked by the Shadow Brokers [34]. These tools were allegedly developed by Tailored Access Operations (TAO), an elite hacking division in the NSA, also believed to be one and the same as the Equation Group [49]. The Shadow Brokers gained access to these tools and released them publicly in April of 2017 [22]. Hackers were then free to use these incredibly sophisticated cyber weapons to spread WannaCry. This attack proved how devastating these weapons can be when publicly available.

Some of the tools leaked by the Shadow Brokers appear to have been available to other hacking groups before the leak, however. In 2019 Symantec found that the Chinese group APT3 had used some of these tools 14 months before they were leaked by the Shadow Brokers, but these tools were also slightly different indicating that they might not stem from the same source [67]. While Symantec can not say for certain how APT3 gained access to these tools, one possibility is that the Equation Group have used these tools during an attack in China, allowing Chinese hackers to reverse engineer the tools based on artifacts left behind, thus opening up venues for proliferation of sophisticated cyber weapons.

Another issue can be a form of mission creep, where tools developed for military use are repurposed for use in civilian law enforcement. This is happening along the U.S.-Mexico border, using tools developed for military use in Iraq and Afghanistan [44]. This seems well-intentioned, but could over time help erode personal freedoms in peace-time, as well as possibly creating a chilling effect on free speech.

2.2.2 The Shape of War to Come

In the last few years have have been several highly publicized cyber operations.

New information led to a new-found understanding of some documents included in the Snowden-leaks [44]. This revealed a highly sophisticated *SIGINT* (signals intelligence) program, called *real time regional gateway*, that allowed coalition forces in Iraq and Afghanistan to intercept mobile phone communications, giving them real-time information on communications and geolocation of known targets.

This program was highly efficient, reducing risk to coalition forces and increasing the accuracy of intelligence gathered on the people that were targeted [44]. At the same time it collected quantities of data too big to be manually reviewed. This lead to a situation where “many civilian lives were lost due to imprecise intelligence” [44].

In a time of US discontent over Russian meddling in the US 2018 midterm election New York Times published a story exposing US cyber operations [58]. These cyber operations were supposedly meant to deter Russian cyber operations targeting the USA, by hacking into the Russian

power grid, possibly preparing retaliatory actions should Russia continue meddling in local affairs [58].

Attacks on power grids have in fact been practiced for many years. Russia was suspected of attacking the Ukrainian power grid in 2015 [57]. This attack utilised similar attack vectors to those of Stuxnet, but the size of the attack was somewhat contained.

Such attacks can be considered a public show of force, and a warning of certain retaliation against any sort of cyber aggression, a modern take on mutually assured destruction. These actions carried out by the cyber superpowers is starting to resemble a *cyber cold war*. This is especially alarming given the apparent disregard for civilians, and the disproportionate danger to civilians caused by the precedent of attacking critical infrastructure such as power grids.

Perhaps the most devastating cyber weapon of all time was NotPetya, released in 2017. The threat actor, commonly known as Sandworm, had gained access to the servers of Linkos Group, a Ukrainian software firm and the makers of the accounting software M.E.Doc, giving them backdoor access to thousands of computers around the world running the software, allowing them to initiate the attack [23].

The weapon was able to self-propagate at a rapid pace, encrypting the devices it infected. In the end, the estimated damages of NotPetya sits at $10 billion [23], a lot of which comes from private businesses caught in the crossfire.

Israel's military published a statement [26] that they had thwarted a hacking operation carried out by Hamas, and then proceeded to bomb the building housing the hackers. While there was speculation that Israeli hackers knocked out Syrian radars prior to an airstrike in 2007 [50], this counterattack against Hamas was the first confirmed incident where cyber operations have been retaliated against with the use of conventional weapons.

This took place in an already on-going armed conflict. That they carried out an airstrike in combination with a defensive cyber operation is interesting, and indicates a strong attribution. It is also likely that the on-going nature of the conflict lowered the bar to initiate the bombing, as Israel could likely repudiate accusations of retaliatory cyber operations, but not a military airstrike.

Rising tension between USA and Iran came to a head after Iran shot down a US unmanned aerial surveillance drone. USA nearly carried out retaliatory attacks using conventional weapons, but the attack was called off in favor of cyber operations aimed at disabling Iranian rockets and missiles [4]. Speculation ensued, as Iran has previously carried out cyber operations against USA, e.g. performing *DDoS* (distributed denial of service) attacks against multiple US banks [72] and destroying company data in a US casino [51].

If tensions between USA and Iran continue to rise and Iran attempts

to carry out cyber operations against USA, we could soon see a response with conventional weapons. It would not be the first example of such retaliation, as seen in the conflict between Israel and Hamas. However, given the ongoing hostility between Israel and Hamas, it would be notable if USA were to carry out a conventional retaliation against Iranian cyber operations, as the first example of such retaliation between two nations, not already engaged in armed conflict. This could set a precedent for what level of cyber attack will be answered with conventional means in the future.

Chapter 3

The Value of Cyber Operations

Espionage and sabotage have been an integral part of international relations for a long time. If executed successfully the victim will never realise that someone has gained access to their sensitive documents. Or in the case of sabotage the target might be unable to hold someone responsible for the attacks. In both cases, however, someone stands to gain from these types of operations. In recent history there has been a shift toward such operations taking place in the cyber domain.

While some cyber operations have been discovered and disclosed publicly, such as Stuxnet, there might be many that have never been discovered, or that have been withheld from the public eye. If the goal of Stuxnet was just to destroy the Iranian centrifuges used in uranium enrichment, why not simply use conventional means, by dropping bombs on the installation? It seems that cyber operations provides more value, with less risk, than many conventional means of attack. Some of the value gained from cyber operations might not be achievable by conventional means.

3.1 Which Factors Make Cyber Operations Valuable?

Different factors contribute to the value of the various types of cyber operations. As an example this section compares cyber collection, or cyber espionage, performed on behalf of the government, with conventional espionage.

3.1.1 Low Risk

Instead of sending operatives undercover into a foreign country, they can operate from their home base. This eliminates elements that make conventional espionage difficult, such as the training and placement of agents. By operating in a foreign nation these agents might risk long prison sentences, or in a few countries capital punishment. By operating from their home country, they are safe from prosecution in foreign countries.

Operatives are also less likely to be identified as an individual, since the foreign nation is severely limited in their surveillance techniques in a

country where they do not control the infrastructure. It is still possible to identify individuals, as was proved by Mandiant [41], but a prerequisite of this was lax security on the part of the identified individuals. Most of the identified individuals reused handles between their private and professional life, left signatures in *malware* (malicious software) and acted in a way that allowed researchers to trace their identities and link them to APT1. However, the report on APT1 created by Mandiant [41] was the first of its kind to be released publicly. It is likely that state-run operations performed after the release of the report have learned from the mistakes that made the report possible.

If an agent performing cyber operations on behalf of their government was identified as an individual, however, the victim nation's options are limited. The agent could be arrested while travelling outside their own country, or be the target of conventional operations in their home country. Such operations, however, would entail their own risks, and likely represent an escalation of the situation where both parties stand to loose more than from the original cyber operation. This could be in the form of lost agents or loss of reputation due to an international incident.

3.1.2 Low Cost

A nation-state will typically try to reduce the cost of operations while maintaining more or less the same value. As already mentioned, cyber operatives can operate from within their own country, instead of being dispatched to another country to carry out operations. This means that operatives do not have to be trained in the extensive skill-set required to carry out a conventional espionage operation in a safe manner, and do not need to incur the direct expenses of travelling.

A traditional operator would have to have some training in skills such as gaining access to highly secured facilities, penetrating security systems, fostering a reliable group of informants and a breadth of other skills required for their operations. Instead of diversifying the operatives' skills in this way they can focus on the skills that will directly affect their performance in cyber operations. Making training quicker, cheaper, more focused, or any combination of the three.

Another factor that helps reduce costs associated with operations lies in the logistics, because operatives and equipment no longer need to be shipped around the world to carry out an operation. Instead of incentivizing employees to steal documents from their place of work, usually by giving them large amounts of money, these documents can be stolen directly from the company server. Instead of smuggling these documents out of the country using diplomats, or other, more nefarious, means they can simply be sent through the Internet using FTP or existing backdoors previously used to gain access to the servers. Cyber operations can be used to exfiltrate terabytes of documents, meaning it is often the better option for effectively exfiltrating large amounts of documents.

3.1.3 Anonymity

Another factor that helps explain why cyber operations are so prevalent is related to the attribution problem. Cyber operations are complex and in the context of espionage no government wants to be caught with their hands in the proverbial cookie-jar. Hence they do their best to avoid detection, and to remove any evidence left behind, so that they can operate with anonymity.

While government agencies will often be less than forthcoming with their intelligence, indicators of compromise can often be guarded as company secrets among the intelligence community as well, contributing to attribution complexity. An example of this was seen in 2018 when Visma suffered from a cyber attack. They hired Recorded Future to investigate the attack. The published report from the investigation claims that "we assess with high confidence that these incidents were conducted by APT10" [29]. It did not take long before other security researchers made claims that the attack had been misattributed, claiming it was APT31, not APT10 [8]. This claim was apparently based on information that was not available to Recorded Future at the time they were working on the report [63].

One takeaway from this case is that attribution is not challenging. There is an overlap of factors that might point to several actors at the same time, making successful attribution about managing the uncertainty of all indicators studied. Operatives will often make use of attack infrastructure that they control, but can be hard to trace back to them. This infrastructure might, even physically, be inside the country they are attacking, and several hops away from the operators themselves.

Successfully tracing a cyber operation to the individual operatives that carried it out can be near impossible, and only rarely of any practical interest. Tracing a cyber operation back to the government that is responsible is often easier, but there are factors that can make this harder. However, these two forms of attribution are not always necessary.

The easiest form of attribution is to look at how an operation is performed, then compare this information to that gathered from other known operations. Based on this information it is often possible to say with some degree of certainty if two, or more, operations were carried out by the same threat actor, often an APT. This is often done in a structured manner which is covered in Section 5.1 below.

3.1.4 Relative Ease and Speed of Operations

The last factor of prevalence is that performing cyber operations is relatively quick and easy. In conjunction with the low costs associated with cyber operations, the relative ease and speed of cyber operations are key reasons why they are so accessible, even for countries, not generally, associated with a highly developed foreign intelligence and sophisticated espionage.

Part of this is related to the lower costs associated with cyber operations, compared to conventional operations, another part is due to accessibility of

required hardware and software. For basic operations no special hardware is required, and software is just as easy get a hold of. There are many distributions of Linux geared towards hacking and penetration testing, e.g. Kali Linux. These often come fully prepackaged with most of the tools required. This makes the software easily accessible to anyone willing to learn how to use them.

While the tools and methods for entry are easily accessible to anyone, what separates a successful operations from an unsuccessful one often comes down to the skill and experience of the operators. This could mean developing custom tools, instead of publicly available ones, being able to produce working exploits for target systems, being able to achieve lateral movement as quickly as possible, or any other part of the operation that is crucial for success.

In their *2019 Global Threat Report*, Crowdstrike [13] published statistics for breakout time, i.e. how long it takes threat actors to achieve lateral movement through the victims network after the initial compromise. While there are many many metrics that can be used to gauge a threat actor's sophistication, this is an interesting, and rather novel, one. While it is little surprise that Russia and China are in the top 5 for breakout time, with 19 minutes and 4 hours respectively, the last three spots go to North Korea, Iran and e-crime with 2 hours and 20 minutes, 5 hours and 9 minutes, and 9 hours and 42 minutes respectively. This metric shows that countries like North Korea and Iran can achieve a sophistication in cyber operations that are comparable to larger and more technologically advanced countries like Russia and China. Again it is interesting to note that western countries like USA and the UK are not included in these rankings at all. It can only be guessed that they would top the list.

3.2 Cyber Operations as Deterrence

One recurring subject when discussing cyber operations is the use of cyber operations for deterrence. One example of this is when, in 2019, the NATO secretary general, Jens Stoltenberg made the statement that "[f]or NATO, a serious cyberattack could trigger Article 5 of our founding treaty. This is our collective defence commitment where an attack against one ally is treated as an attack against all." [65].

Article 5 of the NATO treaty is the collective deterrent supposed to protect signatory nations against foreign aggression and war. In addition, as shown in Section 2.2, NATO has previously defined cyberspace as a domain of war. As such, invoking article 5 in retaliation against cyber operations makes sense. What form such retaliation would take, however, is not clear.

These retaliatory actions could take one of three forms. They could be carried out entirely in the cyber domain, entirely in the classical domains of war, or as a hybrid operation, in both cyberspace and the traditional domains. One difficulty that would likely present itself when attempting to retaliate using conventional means, i.e. traditional military force, is that

it might seem disproportional, thereby reducing public approval of such measures.

While cyber operations can have severe consequences for both health and public security, they are often covert and largely invisible to the general populace. Any retaliation using traditional means would therefore represent a severe escalation of the conflict, at the very least in the eyes of the public. These problems are further compounded by issues that have previously been covered, such as the difficulties of establishing the identity of the attacker, as discussed in Section 3.1.3.

However, if covert cyber operations are never retaliated against with anything but covert cyber operations the deterrent effect might not be adequate. Classic deterrence theory holds that to deter someone from attacking you, e.g. prevent a cyber operation, they must be convinced that you will cause them pain, financial cost, or diplomatic cost, and that these consequences can be avoided by not attacking you [9]. Extrapolating from this we can say that the cost of retaliation, as felt by the attacker, must be greater than the benefits of the attack. However, as long as nation-states do not publicly reveal their cyber capabilities their ability to retaliate against any attack might be underestimated, thus decreasing their capability to successfully deter an attack.

The US Cyber Command seems to understand that deterrence capabilities must be openly communicated. This can e.g. be seen by the press releases about intrusion into Russian power grids [58]. However, while the overt threat of cutting access to power can have a major deterrent effect, if they were to make good on those threats it would be an attack against civilian infrastructure. One casualty will likely be civilian hospitals, that may, according to Article 18 of the Geneva convention, "in no circumstances be the object of attack" [68].

3.3 Regulations on Economic Cyber Espionage

Cyber espionage at the level of national intelligence can be separated into two kinds of operation. One part is akin to traditional espionage outside of the cyberspace, i.e. espionage traditionally aimed at political or military information to further the spying nation's intelligence agenda. The other is economic espionage, infiltrating industry and businesses that are not of national importance and do not hold any national secrets. Such espionage might seek information on business contracts or negotiations, policy papers, internal memoranda or intellectual property. This information is valuable and can be leveraged in order to advance local industries by reducing the cost of independent research and development of new products or methods, undercutting competitors or even beating them to market with new products.

In 2015, USA and China announced an agreement whereby they "would [not] conduct or condone economic espionage in cyberspace" [45]. This agreement occurred with neither country admitting to such practices, even though China is strongly attributed to such operations [41] and USA's

alleged history of attacking civilian infrastructure, and certainly possessing the means to conduct such economic espionage [49, 54].

This agreement between China and the USA does not make any mention of traditional espionage [45], and presumably not any mention of cyber espionage geared towards traditional targets of espionage. This is likely not a coincidence, and there can be various alternative explanations for this.

- Cyber espionage in the form of traditional espionage is simply not a problem as local intelligence agencies are adequately positioned to stop any and all attempts at gaining access to sensitive information. This does not seem to be a likely explanation.
- Most countries have laws against espionage, however these laws already have limitations in the field of traditional espionage where spies can operate with diplomatic immunity. In cyber espionage the operatives can work from within their own borders, meaning the target is unable to prosecute or interfere with the operation outside of cyberspace, and any attempts at governing such behaviour outside of cyberspace is futile. This is likely a part of the explanation.
- The value gained from cyber espionage is simply too high to be relinquished. There exists a form of silent acknowledgement that both parties can continue operations in cyberspace, but they will continually attempt to thwart the other nation's operations in cyberspace, and deny that any such activity takes place. This is also likely to be part of the explanation.

The most likely explanation seems to be a combination of the last two.

3.4 Paris Call for Trust and Security in Cyber Space

In 2018, at the UNESCO Internet Governance Forum, the French president Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace, which proposes a set of cybersecurity principles [43]. The agreement aims to create common principles for securing cyberspace whereby the signatories commit to help each other and implement measures to achieve several goals. These goals are expressed below.

> Increase prevention against and the resilience to malicious online activity; Protect the accessibility and integrity of the Internet; Cooperate in order to prevent interference in electoral processes; Work together to combat intellectual property violations via the Internet; Prevent the proliferation of malicious online programmes and techniques; Improve the security of digital products and services as well as everybody's "cyber hygiene"; Clamp down on online mercenary activities and offensive action by non-state actors; Work together to strengthen the relevant international standards [43].

As of June 2020, notable non-signatories include many of the world's foremost cyber powers, the USA, Israel, China, North Korea, Russia and Iran [52]. This is not unexpected, given the value these countries appear to attain from cyber operations and the activities that the Paris Call would like to curtail. The Great Firewall of China reduces the accessibility of the Internet, Russian hackers have been revealed to interfere in foreign elections [17] and the U.S. National Security Agency (NSA) have been caught inserting backdoors into the cryptography that secure Internet transmissions [5].

Chapter 4

Threat Agents

4.1 What is a Threat Agent?

As seen in Chapter 2 and Chapter 3 cyber operations are highly valuable to many nation-states. Cyber operations are a low-cost, easy and effective way to achieve goals that, 30 years ago, would require putting agents through extensive training and sending them on, potentially, dangerous operations in foreign countries. Such agents are still at the core of cyber operations, but they no longer have to go through the rigorous training to operate in foreign countries. As the resources of a nation-state is no longer necessary to become a proficient agent, other parties have also started performing cyber operations.

By the definition of cyber operations given in Section 2.1 cyber operations are performed with a specific objective or intent. This implies an actor, typically known as a threat actor or threat agent, with the capabilities and intent to produce an attack. There are many ways to categorize threat actors, e.g. they can be categorized by their role in the operation. A threat actor could be a *developer* of malware or an *operator* of a botnet or responsible for any of the other roles involved in a cyber operation.

When categorizing threat agents an interesting and important aspect is the allegiance of the agent. The agent might be working for a nation-state. The agent might also be autonomous, acting in pursuit of individual interests or work on behalf of somebody else's interests, or both of these at the same time. Working on someone else's behalf could be a simple arrangement where the agent is providing services for a fee, or even a stable income, or the agent could be working out of ideological convictions.

When talking about a threat agent working on behalf of another party, that party is referred to as a *sponsor*. Sponsors might be incapable of performing such attacks themselves, either because they lack relevant skills or the right equipment, or the sponsor might attempt to distance themselves from the attack. In the latter case the sponsor will typically pay an operator to carry out the attacks, these attacks might be possible to trace back to the operators' attack infrastructure, but to trace them back to the sponsor will be a lot harder.

4.2 Categorization of Threat Agents

Categorization of threat agents can be done in any number of ways, and several taxonomies have been created in order to properly categorize these cyber threat agents [2, 11, 12]. While this work provides a highly detailed set of actors appropriate for some uses, a less granular categorization is presented below.

While definitive attribution is hard, categorization following a scheme like the one below can be helpful. It will not explain who perpetrated the attack, but understanding how the attack was performed, and knowing which data the attacker targeted can inform categorization which, in turn, can help direct further investigations.

State actors. Typically referring to national intelligence agencies. Operations carried out by a state actor are typically performed in support of that nation's strategic goals. State actors are competent, well-funded, patient and highly organized. State actors usually have access to a significant network infrastructure, both for listening in on internet traffic and carrying out operations, and reliable access to working computer exploits in order to carry out operations. Such operations can be highly advanced, with teams working around the clock for high value targets, typically far surpassing other threat actor categories in their capabilities.

Commercial actors. Commercial actors can perform cyber operations in order to support an, otherwise, legitimate business. Keeping up with a competitors R&D through digital industrial espionage or securing their own technological advances through network defence might be of equal interest to commercial actors who perform such operations. The 2018 attack against Visma was quickly deemed to be a "classic case of industrial espionage" [27]. Often, however, the target victim of such attacks might attempt to keep the attack silent, rather than suffer potential decreased reputation as a consequence of being a vulnerable target for hackers.

While there are accusations of businesses performing cyber operations or willingly enabling state actors to perform cyber operations through their systems, these accusations are rarely followed by successful legal action. While allegations against companies like Huawei and ZTE could have some merit, other allegations against corporations seem more like conspiracy theories, e.g. the conspiracy theory that makers of antivirus software engage in distributing computer worms to increase sales if their antivirus products.

Organised criminals. Organised criminals conduct cyber operations in support of, or in direct combination with other illegal activities. This is usually in the form of fraudulent behavior, but could also be buying and selling of illegal goods and other illegal activity.

Idealists, hacktivists. Such actors are typically idealistic in the sense that they perform operations in support of an ideological belief. Some notable actors are Wikileaks, Anonymous, and Anonymous' related groups. These groups are typically not well-funded, and do not have access to the same kind of infrastructure that state, commercial actors, or even organised criminals, do.

On a technical level these groups are typically not as competent as the previous categories of threat actors, but they can still cause a lot of damage. Hacktivists often use rather simple forms of attacks, such as DDoS attacks, or SQL injection [69]. DDoS is a simple form of attack that is easy to perform with automated tools. Even though it is a simple form of attack, with a lot of willing participants they can cause a lot of damage. SQL-injections can also be automated with tools, or performed manually. While manual SQL-injections require more skill than automated attacks it is still a fairly easy attack to perform.

Terrorists. As is the case in conventional usage of the word terrorist, terrorists operating in the cyber domain can also be recognized by their use of violence and intimidation. Despite cyberterrorism's prominent role in popular culture, typically portrayed as dangerous and extremely potent, real cyberterrorists do not appear to have reached the capabilities exhibited by their fictional counterparts.

Hackers claiming affiliation with ISIS have claimed responsibility for attacks that apparently never happened [56], released "kill lists" that under closer scrutiny appear to be a selection of public leaks from services such as LinkedIn and Myspace [53]. While their cyber capabilities are far from that of Bond-villains, such behavior still causes fear in the general populace, making them deserving of the brand as terrorists.

4.2.1 Advanced Persistent Threats (APT)

APTs were left out of the classification schema above, as they would not fit neatly into that classification. APTs are highly sophisticated groups of hackers, they are able to gain access to computer systems and exploit them over long periods of time, hence the name. Such attacks are typically highly targeted and tailored to the network it is targeting. APT as a term can apply to several of the categories above, while the terms is often used for state intelligence, cyber armies or state sponsored hackers, it can also apply to cyber criminals.

Another reason is that while approximately 40 APT-groups, numbered APT1–APT40, are being tracked on the Internet, the companies and researchers tracking them are usually from Western countries. This means that not a single APT tracked by FireEye is from a Western country, even though countries like the USA, the UK and Israel are on par, or far more sophisticated than the APTs that are being tracked. The Equation Group, among the most advanced hacking groups in the world, if not the single most advanced group out there, does not have an APT-number, at least not among the publicly available APT-reports from FireEye [20].

Chapter 5

Detecting Cyber Attacks

Properly implemented and up-to-date network defense will guard against many forms of cyber attack. However, examples from the last decade have shown that a sophisticated operation, typically attacks from an APT, can breach the security of a highly secure facility, even managing to cross into an air-gapped network [73], i.e. a network completely disconnected from the Internet. Since these attacks are specially crafted they typically circumvent off-the-shelf security solutions, making detection harder.

5.1 Modelling an Attack

An important tool in detecting sophisticated cyber attacks is attack modelling. These models break down an attack into it's components and makes it easier to analyse how the attack was carried out, or how much information the defender has on a given attack. The immediate benefit of applying such models is a more robust detection, hardening security against future attacks using the same attack vectors. This information when gathered over time and from many attacks, makes it possible to build a profile of different APTs. This, in turn, allows attribution, at least in a limited sense where it is possible to attribute attacks to a group, even if their identity is not known.

There are several models that are intended to model cyber attacks. It is important to note that while these are useful for advanced attacks, simple or opportunistic attacks launched with no clear intent, strategy or goal does not fit into the following models.

5.1.1 Cyber Kill Chain

In 2011 Hutchins *et al.* [28] published an article where they described *the cyber kill chain*. The cyber kill chain, as shown in Figure 5.1, is a model that describes how an APT attack is performed, by splitting it into multiple, distinct stages. These stages form the chain that gives name to the model, each stage reliant on the one that came before. Stopping, or killing, any stage of the attack will also stop the attack. Being able to successfully stop an attack early leads to less consequences for the defender.

An important part of the cyber kill chain is analysing the attacks and using the information gained to further harden the security. After killing an attack in the C2-stage the defenders should analyse the attack through each stage of the cyber kill chain, and make efforts to mitigate vulnerabilities that allowed the attacker access. Analysis should also attempt to simulate the attackers actions further down the chain, in order to harden security at all levels. This allows the defenders to use the persistent nature of an APT against them, mitigating the risk of future attacks along the same attack vectors.

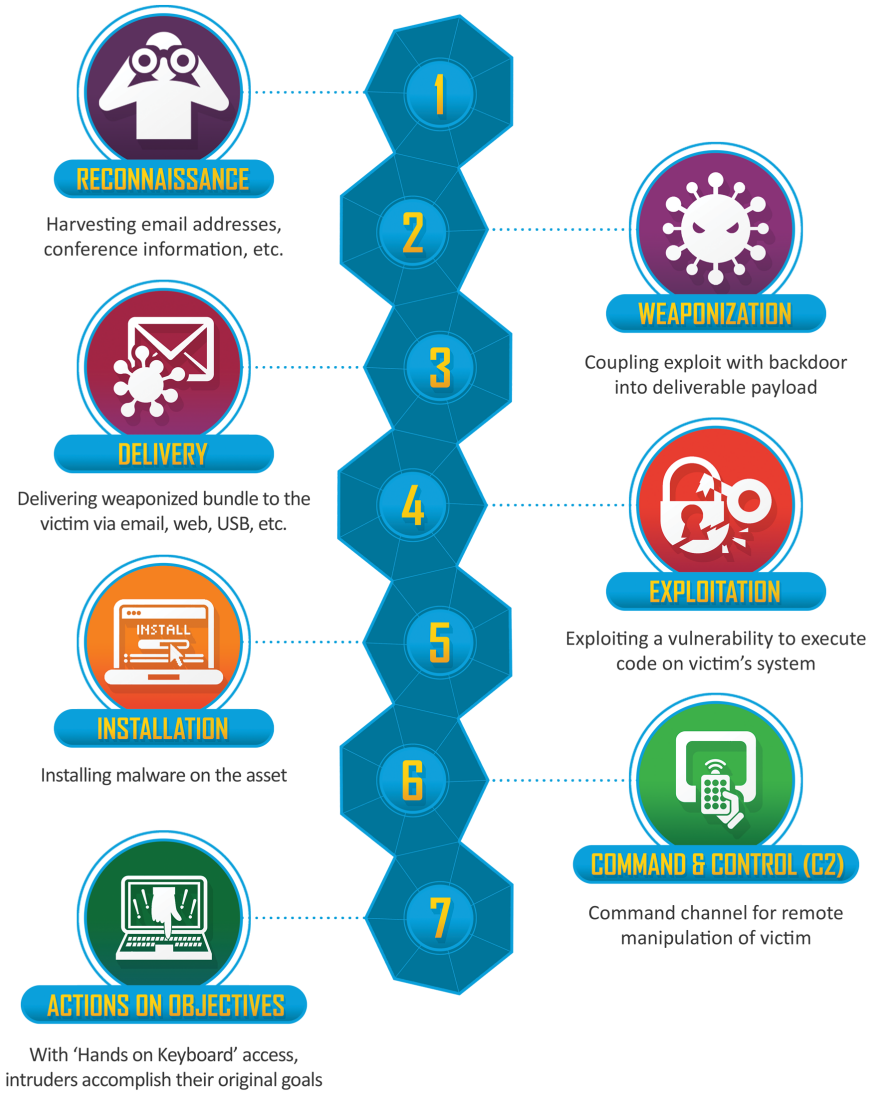

Figure 5.1: Cyber kill chain [35].

Reconnaissance. Identification and selections of targets. Can be performed through crawling of open websites, social media and mailing lists for contact information, social relationships, or other identification that can

be abused in later stages. Can also include scans of target systems in order to look for vulnerabilities.

Weaponization. Preparation of malware, typically an exploit that will install a remote access tool (RAT). This exploit is often delivered in a seemingly harmless file, such as a PDF, Microsoft Office document or an image file. The approach chosen typically depends on earlier reconnaissance of the target.

Delivery. Delivering the malware to the target. The most common ways to achieve this, according to [28] are listed below.

Phishing and spearphishing. These attacks typically take the form of a malicious email. Phishing is often generic, sent to many people at once and usually easy to identify as fraudulent. Spearphishing is typically targeted at one specific person, or at most a few people, where the recipient victims can be thoroughly researched. If the email's content seems relevant to the recipient, contains information that is up-to-date, and possibly arrives at an opportune time it can be hard to recognize as fraudulent. These emails will either contain the weaponized file or a link to download it.

Watering hole attacks. This sort of attack involves compromising a webpage that the target already trusts, or otherwise has reason to trust, e.g. a take-away restaurant they regularly order from. Since the trust is already established the target is less likely to recognize an attack, for instance if the site asks you to download the menu in PDF-format. If the attacker has done research prior to the attack this sort of attack can still be highly targeted, e.g. by serving the malware only to a target IP-address.

Portable media. Distributing CDs and USB-sticks with autorun is still an important way to spread malware. It is possible to deliver the initial infection this way, but more importantly malware that is capable of infecting new USB-sticks is one of several ways an attacker can infect an air-gapped network.

Exploitation. After delivery, this stage triggers the intruder's code. Typically the exploit will target vulnerabilities in the operating system or an application, or it can trick the user into granting additional rights. Actions the user would often have to take includes interaction with Windows user account control, activating macros in an Office document or visiting an infected website.

Installation. Installation of a RAT or backdoor on the victim system. This allows the intruder to maintain persistence.

Command and control. Unless the malware is fully automated an infected host will need to establish an outbound connection to some sort of infrastructure operated by the attackers. This is referred to as command and control (C2). When the connection is established the attackers have full remote access to the compromised host.

Actions on objectives. Finally the intruder has established a foothold and can proceed to take actions in order to achieve their original objectives.

5.1.2 The APT Attack Cycle

In 2013 Mandiant presented the cyber attack lifecycle [41], seen in Figure 5.2. The cyber attack lifecycle is a high-level overview of common parts of an advanced OCEO. The attack lifecycle is divided into eight distinct steps, where the steps between *establish foothold* and *complete mission* are repeated continuously, and not necessarily in the order they are presented here. Below follows a summary and interpretation of Mandiant's general description.

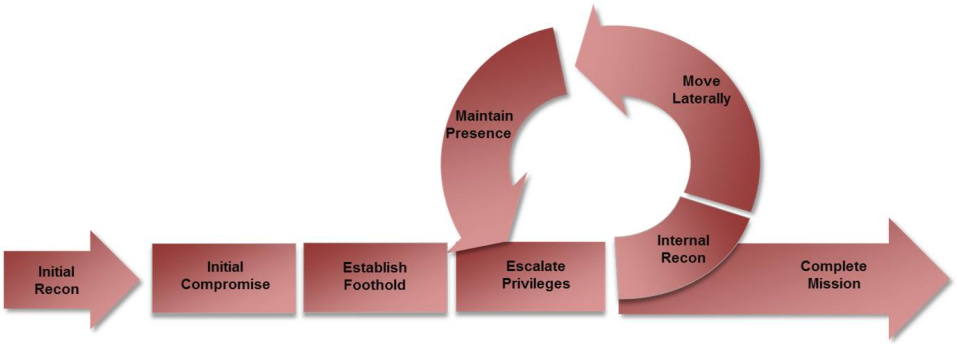

Figure 5.2: Cyber attack lifecycle [41].

Initial compromise. The initial compromise stage covers the methods that intruders use to penetrate a target's network. This might occur in a number of different ways, but the most common way appears to be *spearphishing*. Other ways for a threat agent to gain access might be through removable media, such as USB-sticks, *watering hole attacks*, or exploitation of vulnerabilities on Internet-facing web-servers or public-facing infrastructure.

Establish foothold. In the establish foothold stage the intruders ensure continued access to the target's systems. This is commonly accomplished by installing backdoors, which is malware that can establish an outbound connection from within the target's network. Malicious outbound traffic is often harder to detect and terminate than inbound traffic. Malware for such backdoors can be developed by, or for, the intruder, or it can publicly available.

Escalate privileges. Escalation of privileges is the act of gaining additional access to the target's computers and network. This is done in many ways. Often this is done primarily through obtaining usernames and passwords, especially ones belonging to privileged accounts like local administrators or domain administrators. Escalation of privileges can also be gain-

ing access to PKI certificates or network infrastructure such as privileged computers or VPN client software.

Internal reconnaissance. In the internal reconnaissance stage the intruder maps out the target's internal network to collect information about the environment and locate servers that might hold interesting documents, such as file servers, email servers or domain controllers. In this stage an intruder might use built-in operating system commands and tools. If these tools are also used by the system administrators in regular day-to-day operations it might be hard to distinguish legitimate use from an attacker.

Move laterally. In most cases, the system the intruders first gain access to does not contain the data they are after. In order to gain access to valuable data, the attackers move laterally through the network. Lateral movement typically happens by using credentials obtained in the earlier stages of the attack, or by pass-the-hash tools they allow intruders to leverage a hashed password without cracking it first.

Maintain presence. The stage of maintaining presence covers the methods whereby intruders ensure continued access and control over the compromised systems from outside the network. They might continue to install new backdoors, even ones from a different family of malware than the initial backdoor, which ensures multiple points of entry for later exploitation of the systems. They might also install backdoors from different families of malware, which will make it harder for the target to locate and remove their points of access from the network. Using several command and control addresses makes tracking their operation more difficult for the target. If they gain access to legitimate PKI certificates or credentials they can also maintain presence by masquerading as legitimate users.

Complete mission. In this stage the intruder has gained access to valuable data, such as intellectual property, business contracts, policy papers or internal memoranda, and need to exfiltrate it. This is often achieved by compressing the data, using tools like RAR, ZIP, or 7-ZIP, frequently password protecting them, and then transferring it out of the network using e.g. FTP or existing backdoors. Such traffic might be encrypted in order to make the operation harder to detect, or to hide it from anyone surveying the network traffic.

5.1.3 Pyramid of Pain

In 2013 Bianco wrote about his model, the pyramid of pain [6]. His model was inspired by the large amounts of IOCs in Mandiant's report on APT1 [41] and how best to use them for network defense. The pyramid of pain is a way to rank IOCs based on how much pain successful detection will cause the attacker. The pyramid itself, as shown in Figure 5.3, is made up of six levels, from Hash values to TTPs, with corresponding pain levels.

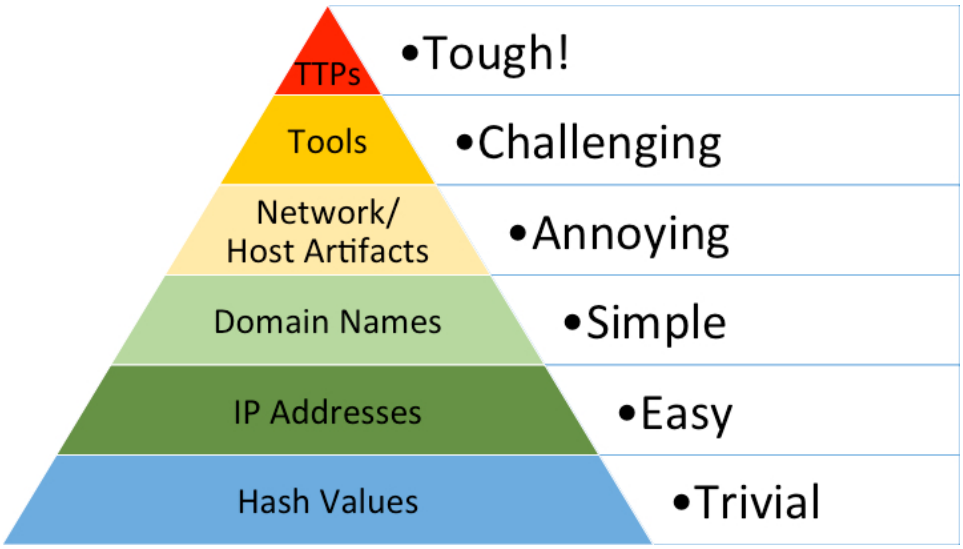

Figure 5.3: Pyramid of pain [6].

Hash values. These IOCs are the most trivial. Hash values are incredibly accurate when used to detect multiple instances of the same malicious files, e.g. a malware sample. However, since hash algorithms calculate a unique value from the entire input it is a trivial task to change a file so that it will not be detected.

An exception here is for fuzzy hashes. These are hash algorithms that generate similar hash values for similar input. Bianco argues that these hashes fit better in the Tools level of the pyramid, since "they are more resistant to change and manipulation" [6].

IP addresses. One of the most fundamental indicators, and an integral part of any traffic sent through the Internet. IP addresses can be an accurate indicator, but there are many of them, and an attacker can easily change his IP address.

Domain names. Unlike IP-addresses a domain name must usually be registered, paid for and hosted somewhere. However, it is possible to register for free domains, or buy them with stolen, untraceable money from registrars with lax registration standards. In addition, new domains can take a couple of days to propagate throughout the Internet, making changes slightly harder than IP addresses.

Network/host artifacts. These are observable indicators that can be observed during or after an attack. While any observation on the network or on the endpoints could be considered an artifact, the only interesting ones are the ones that can identify malicious behavior, as opposed to legitimate use. Network artifacts can be e.g. URI patterns, distinctive HTTP user-agents or C2 information embedded in network protocols. Host artifacts can be e.g. registry keys or values known to be created by specific

malware, files dropped in certain places or names used by malicious services.

This is when detection starts to make a difference for the attacker. In order to avoid detection the attacker will first have to figure out what the defenders detect them on, and then make the appropriate changes to avoid detection, e.g. recompile a tool to use a different user-agent.

Tools. Software used by the attackers, specifically software they bring with them, and not the tools already present on the target computer. This could be backdoors, password crackers or any other software for use in the attack, or post-compromise in order to exfiltrate data.

This is when it starts to get painful for the attackers. If the defenders are able to consistently detect their tools they need to spend a lot of time in order to find or create new tools, and become proficient with them.

Tactics, techniques and procedures (TTPs). At this level the defenders are no longer detecting merely the single tools or artifacts, but are capable of detecting the attackers by how they operate. This could mean detecting an attacker by how they perform a spearphishing attack, i.e. what sort of file dumps the RAT or how they routinely chain together multiple steps in order to perform an operation.

Being able to detect at this level is a big hit against the attackers. They can no longer just ecompile their tools, or get new ones. Since the defenders can detect an attacker by how they operate the only way to avoid detection is to change behavior and find another way to achieve the same goals. This can be really hard.

5.1.4 DML and Semantic Threat Modelling

In 2014 Stillions [64] wrote about the Detection Maturity Level (DML) model. The DML does not model the actions of an attacker, but rather how successful the defender is in detecting cyber attacks. This model uses a lot of the same language as the Pyramid of Pain, presented above, and is a way to gauge how successful the defender is at detecting attacks at the different levels of pain, this is what Stillions calls *maturity*. This maturity is not measured in the amounts of intelligence the defender is able to obtain, but rather in how well it succeeds in using this intelligence for network defense. The model will be presented below.

The DML model, as it was first proposed by Stillions, was divided into 9 maturity levels, DML-0 through DML-8. In [10] Bromander *et al.* expands the DML model to include a tenth level, DML-9, which represents attribution. This expanded model can be seen in Figure 5.4. DML-0 is the maturity of a defender that does not have any detection capabilities. Above this baseline level the lower levels are the most technically specific, while the upper levels are the most technically abstract. As such, as noted in [10] the lower levels provides good precision, i.e. if you detect a malicious IP-address there is not much room for interpretation. The upper level

provides more robustness, i.e. they allow for robust detection that is not based on simple technical indicators that can be changed in a matter of minutes. However, the higher levels are more open for interpretation as e.g. different attackers can have similar techniques, introducing uncertainty in the attribution of the attack. DML levels 1 through 9 are summarized below.

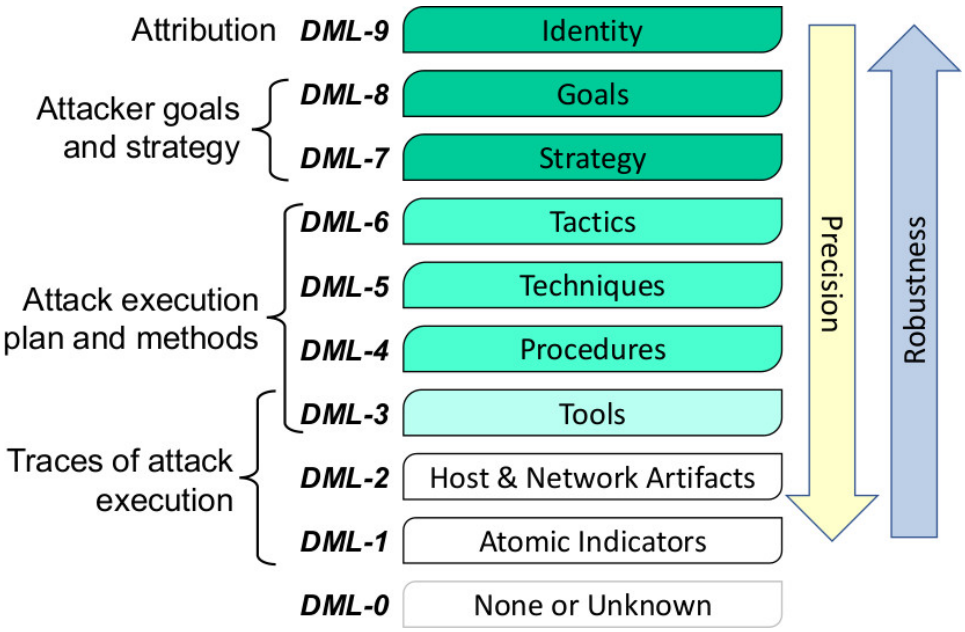

Figure 5.4: The expanded detection maturity level presented in [10].

DML-1 Atomic indicators of compromise. The very basic elements of detection received from intel feeds. Such elements can be IP-addresses, domain names or strings used in malware binaries. These basic elements change rapidly, and have a small window of usefulness wherein they can be used as IOCs.

DML-2 Host & network artifacts. These are indicators that can be observed during or after an attack, i.e. it can be collected by endpoint and network sensors.

DML-3 Tools. While tools are not as volatile as indicators collected at lower levels of detection, they are still subject to change as they are continually developed by the attacker. Detection of tools fall into two categories. One is being able to detect the tools as they are transferred over the network or as they lie in the file system, the other is detection of the tool's functionality. Operating at DML-3 means being able to reliably detect an attacker's tools even after minor changes to the tool itself, or the host and network artifacts it leaves behind.

DML-4 Procedures. Procedures refers to a sequence of individual steps. DML-4 is being able to detect the procedures an attacker performs methodically and multiple times during an intrusion. According to [64] procedures "are one of the most effective ways of detecting adversary activity".

DML-5 Techniques. Techniques are the specific ways of executing a single step in an attack. Such techniques can be so specific as to be nearly unique.

DML-6 Tactics. Tactics refers to how an attack was designed. Operating at DML-6 means to be able to recognize a tactic regardless of the specific tool, technique or procedure was used to execute it, or the artifacts and atomic indicators left behind after the attack.

DML-7 Strategy. Strategy means the non-technical, high-level plan of attack. There are many ways to achieve the attackers goal, the strategy is how the attacker intend to achieve it. DML-7 and above are non-technical, and DML-7 and DML-8 are subjective in nature. This means that these levels can only be inferred by analysis of the attack or attacks, but possession of intel on this level can be extremely valuable for the defender.

DML-8 Goals. This is the non-technical, high-level goals the attacker intend to achieve. Depending on the attacker the individual operator that performs the attack might not know what the ultimate goal is.

DML-9 Identity. The identity of the attacker. This could be the name of an individual, a group or a nation-state. If it is not possible to identify the attacker it can still provide value for the defender to link an attack to other attacks performed by the same attacker.

Chapter 6

Bugs and Vulnerabilities

Computer bugs are an unavoidable part of modern computer software. At their worst bugs are the cause of vulnerabilities in computer systems, errors so significant that they can be exploited by others to leak data, inject code into the computer, or even take control of it entirely. Removing bugs will often mean blocking the attack vectors that are exploited by malicious hackers, whether they be state intelligence or some less sophisticated hackers.

6.1 Dealing With Bugs

The majority of bugs and vulnerabilities are handled during development, simply because developers of software have a vested interest in making sure that their software is as free of bugs as possible. This is both for making sure that the software is secure, but also to make sure that it runs as intended. For these reasons the most important time to secure software is in the development phase, this is also the cheapest time to handle bugs. Making security a priority in the development of software is often referred to as built-in security.

Built-in security is important in modern software, but security efforts do not end at deployment. Modern software is continuously developed and improved, these efforts improve security and functionality over time, but they also run the risk of introducing new bugs and vulnerabilities. Therefore securing software and computer systems need to be a continuous effort.

Vulnerabilities are discovered in a multitude of ways, by independent researchers, in the aftermath of attacks, through cooperation with *CERT*-groups (computer emergency response teams) etc. One strategy to help increase security after release is crowd sourcing of vulnerability hunting, so-called bug bounties. Companies offer a monetary reward to researchers who report vulnerabilities responsibly for fixing. Typically there are pre-approved *rules of engagement* that regulate e.g. what tools and techniques can employed by the researchers, in order to ensure the integrity of the company's computer systems.

6.2 Vulnerability Life Cycle

As vulnerabilities are found and patched, new ones are continuously introduced. Some vulnerabilities are discovered and some are never. When a vulnerability is discovered by someone, that vulnerability might be disclosed, sold, exploited, or kept secret for later use. Newly discovered vulnerabilities often prove the most ripe for exploitation. The most successful forms of malware often start by exploiting software vulnerabilities that are not publicly known, known as *zero-day attacks*. Bilge and Dumitraș [7] did a study of zero-day attacks, looking into how they evolve throughout the vulnerability life cycle model.

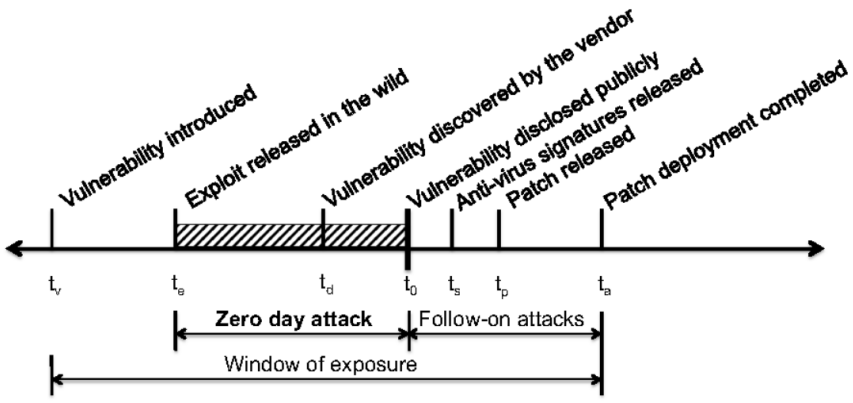

Figure 6.1: Vulnerability life cycle, as presented in [7]

The vulnerability life cycle model was first introduced in [3]. The version used in [7] (see Figure 6.1) change the names of the phases, and presents it as follows.

- Vulnerability introduced
- Exploit released in the wild
- Vulnerability discovered by the vendor
- Vulnerability disclosed publicly
- Anti-virus signatures released
- Patch released
- Patch deployment completed

These phases do not always occur in the same order, occasionally multiple phases can be entered at the same time. A key identifier of zero-day attacks is that the exploit is released in the wild before it is publicly disclosed.

Out of 18 zero-day vulnerabilities included in their study, 15 targeted less than 1000 computers, this appears to confirm the hypothesis that zero-days are primarily exploited by sophisticated attackers, e.g. nation-states performing targeted cyber operations. These zero-day attacks can also

last for a very long time, the attacks studied by Bilge and Dumitraș lasted between 19 days and 30 months, with an average duration of 312 days [7].

Later, after vulnerabilities were publicly disclosed they found a drastic increase in attacks targeting the vulnerability. The number of attacks in the *follow-on attacks* window (see Figure 6.1) rose by a number between 2 and 100 000 times when compared to the number of attacks prior to public disclosure. The time after public disclosure is therefore a critical period where vendors need to develop and release a patch, and vulnerable targets should take action to mitigate risk of a successful attack, or consequences of a successful attack.

Chapter 7

Security in Software and Hardware

In 2007 Syrian radar systems were disabled shortly before an airstrike by Israeli bombers of a suspected nuclear installation. This lead to suspicions that Israel had activated a hidden kill-switch, installed by the vendors, in order to avoid detection before the attack [1]. While this kill-switch has never been confirmed to exist, or to have been activated, this is still a very real possibility faced by any nation who buys hardware and software for their critical systems from another nation.

In August 2018 USA banned government use of technology created by Huawei and ZTE, after having considered the companies a security risk since 2012 [31]. Australia announced that Huawei and ZTE were banned from supplying 5G technology, over concerns of national security, shortly thereafter [62]. Many other countries implemented similar restrictions in the months that followed, or are on the verge of doing so.

This streak of bans seems motivated by a newly implemented Chinese law that gives the government the power to compel people and organizations to assist in acts of espionage [55]. The legislators in many countries appear to be afraid that the Chinese government will leverage Huawei's position in the market of modern information and communications technology (ICT) to spy on their countries.

Whether or not Chinese companies engage in this activity has not been proven, for now it is merely a concern legitimized by Chinese law. However, the Snowden-leaks [24] showed that the NSA have been intercepting computer network devices with, or without, the knowledge of the American vendors. The NSA would then implant the devices with a beacon, hardware that would *phone home*, i.e. create a network connection that would give the NSA backdoor access to the network they were installed in. The device would then be repackaged with a factory seal and sent to the customers, all over the world.

Even if these vendors were not aware of the actions of the NSA, the Snowden-leaks proved that other big companies had been cooperating with NSA, making the U.S. government culpable of the same behavior they are accusing China of committing. If a vendor is aware of such operations,

or they are collaborating with nation-states the vendor can be deemed as untrusted by other nations, or by businesses. This raises the question, investigated in [39], is there any way to verify and build trust in ICT equipment, or any other product, from an untrusted vendor?

7.1 Public-Private Collaboration in Cyber Operations

Collaboration in cyber operations between governments and private companies can occur in under a wide range of circumstances, and take many different forms. Jøsang distinguishes between three forms of collaboration, active, passive and forced [30].

If an intelligence agency hacks into company servers to carry out a cyber operation, e.g. for the purposes of a supply chain attack, without the company's knowledge this does not constitute collaboration, i.e. collaboration require that the company is aware of the operation. In the case of active or passive collaboration this means that the company must have made a conscious and voluntary choice about their own action or inaction in relation to the operation.

Active participation is an example of the company participating or facilitating an operation, e.g. an American company knowingly installing an NSA backdoor into their product, fully understanding what they are doing. Passive collaboration occurs when the company is aware of the operation, but do not take the actions available to them to hinder it, Jøsang exemplifies this with "when RSA discovers a vulnerability in one of their security products which they know can be exploited by NSA, and they do not attempt [to] remove that vulnerability" [30].

Forced collaboration means the company being coerced into participation. An example of this came in 2016 when the U.S. government demanded, on the basis of law, that Apple create a way to disable security features of an iPhone, owned by the perpetrator of a terrorist attack in San Bernadino [42].

Jøsang [30] also notes that through collaboration with businesses in the technology sector governments can significantly increase and simplify their capabilities for cyber operations. He writes about four types of collaboration between governments and partners in the IT sector, collaboration with operating system vendors, CPU and microchip vendors, system vendors and cloud providers. If granted access to a company server there is no need to develop new attacks or exploitations, completely bypassing one of the biggest challenges in cyber operations. Other collaborations, like that between NSA, Google, Facebook, Apple, and others technology companies, under the PRISM-moniker [25], gave NSA access to significant amounts of data, for surveillance.

Governments can benefit from collaborating with a diverse set of companies, working in different fields. Modern operating systems are large and complex pieces of software, so large and complex that they contain any number of undiscovered bugs and vulnerabilities. As vulnerabilities become publicly known, and exploits are made available on the Internet

any company that does not update their systems in a timely manner is vulnerable.

Even as software updates are becoming increasingly automated, the updates are often opaque to the end-user. There is, however, still a strong incentive for businesses to keep their systems up-to-date in order to avoid malware infections. These updates allow the vendor to change the operating system at will. If vendors are cooperating with national intelligence this gives the agencies an easy way to carry out cyber operations on target systems, e.g. by bundling a backdoor into a system update. This also applies for vendors of modern mobile phones, giving agencies access to the miniature computer, photo camera, and sound recorder most people carry around daily.

Collaboration with hardware vendors open different opportunities. Due to the interaction between the software and hardware levels of a computer system, it could be possible to include extra functionality in the latter in order to perform unexpected operations on a compromised system, such as additional or alternative functionality in response to calls from the operating system.

An additional 1000 transistors on a microchip would be enough to implement a kill-switch [1], allowing vendors or their partners to knock out affected systems remotely. With even consumer-grade CPUs containing billions of transistors [33] finding such a kill-switch is akin to finding a needle in a haystack.

Another form of hardware is the TPM (trusted platform module), a security chip that can support the verification of the integrity of low-level software, such as the BIOS and kernel, before a computer starts the boot-process. In some cases it could also limit a user from configuring the system freely. According to Jøsang "[i]n case an exploit has been built into the BIOS or kernel of a computer equipped with TPM, then it might be impossible for the owner to remove those exploit" [30].

Involving system vendors in such collaborations gives intelligence agencies the option to add additional chips on the motherboard. While NSA is known to perform similar action on hardware, either shipped to them or intercepted in shipping [24], as Jøsang says such actions "would probably be much simpler when done at the assembly line of companies like Dell or HP, or during customization by the local distributors" [30]. Collaborations on this level would also likely mean that additional chips could be more tightly integrated in the design of the product, potentially making it harder to discover.

7.2 Trust That Can Not Be Verified

"Trust, but verify" is a well known Russian proverb. Before the digital revolution verification was as simple as picking something apart and reassembling it. In the digital age things are no longer quite as simple. A program that has been compiled can not simply be decompiled into the original source code. There are several ways of analysing a program,

these vary in effectiveness, measured both in time spent, and the ability to discover malicious behavior.

While bugs and vulnerabilities in hardware is not a new concept, the amount of vulnerabilities discovered in hardware has increased in the last few years, with Rowhammer [61], Spectre [32], and Foreshadow [70] being a few notable examples. This means that the hardware, as well as the software, will need to be verified as trustworthy.

7.2.1 Static Analysis

Open-source software make the source code available, so anyone can audit it, i.e. look for malicious or insecure parts that could be a security risk. This is known as static analysis, and it is a time consuming exercise. Dowd *et al.* suggest skilled auditors average between 100 and 1000 lines of code an hour [16]. Going thorough verification of all commonly used tools in this manner is both expensive and time consuming, likely prohibitively so for many organisations.

A more time-efficient form of static analysis is the use of signatures, i.e. a set of instructions that are associated with malicious behavior. When a signature is recognized in a piece of software it might be malicious, depending on how accurate the signature is it can produce false positives. The success of such techniques has led to developers of malware applying obfuscation techniques, e.g. by encrypting code, and decrypting it in runtime. New techniques are developed over time, such as heuristic detection. Where signature based detection is strictly binary, heuristic detection checks multiple indicators before determining if the software is benign or malicious.

7.2.2 Dynamic Analysis

As static analysis can be time-consuming, or inaccurate, due to obfuscation techniques, an alternative technique is dynamic analysis, i.e. analysing the program as it is running. This form of analysis does, however, come with its own set of drawbacks, e.g. a lack of observable malicious behavior does not prove there are not any malicious parts. The program could wait a long time before it runs any malicious operations, or it could be waiting for some external input.

There are two main ways to carry out dynamic analysis, one is where the software is analysed on a live system, connected to the Internet. This can be called unrestricted execution [36]. Unrestricted execution comes with the most serious drawback, namely that any malicious behavior exhibited by the software is free to execute as intended, potentially infecting other parts of the systems.

An alternative is to run software in an emulated or virtualised environment. Such methods allow for restricting malicious behavior, but is subject to slower execution compared to unrestricted execution, and evasion techniques, e.g. software not executing malicious code if it recognizes it is running in a virtualised environment. As analysis in

virtual environments is not usually run for long periods of time, at least compared to a live deployment, waiting can also be an effective way to evade detection.

7.2.3 Reverse Engineering

Reverse engineering can also be a way to analyse software. The techniques used in reverse engineering can be further broken down into static and dynamic analysis.

In order to perform static analysis of software it is often necessary to disassemble or decompile the executable binary file. Disassembling means translating the binary code into human-readable code, i.e. assembly code, whereas decompilation means attempting to translate the binary back into its original source code. Neither of these restore variable names, comments or similar metadata, making these techniques more time-consuming than static analysis according to the arguments in Section 7.2.1. This form of analysis can also be made harder by obfuscation techniques.

By using debuggers it is possible to analyse the operations carried out by the program as it is running, as well as its internal state every step along the way. Debugging software is a good way to work around the limitations of static analysis of disassembled software, but carries some of the same risks associated with dynamic analysis. However, being able to change the internal state of the program as it runs can make it possible to trigger hidden functionality in order to study it.

7.2.4 Hardware

Hardware can be analysed in the same ways as software, albeit using different techniques. Many of the same limitations remain, however, as instead of analysing hundreds of thousands of lines of code, hardware require the analysis of hundreds of millions of logic gates. While each logic gate performs a very simple operation, it is not an easy feat to understand the operations of the chip by just studying the logic gates [37].

Moreover, because of the structure of a microchip, i.e. the logic gates being spread over multiple layers, it is next to impossible to do a static analysis without reverse engineering the chip, a process that destroys the chip by physically removing the layers that contain the logic gates [1].

Even if, with the goal of securing national infrastructure, nations were willing to loose some money by destroying the occasional chip, under the assumption that all the chips are the exact same, i.e. one chip does not contain malicious behavior that is not exhibited by all other chips, it might not help. According to Lysne "[f]ully reverse engineering a modern complex chip to the extent that all details of its operation are understood, down to the impact of every bit-level gate, is practically impossible, given the amount of effort it would require." [37].

Dynamic analysis is not a solution to these problems, either. Lysne writes that there is two ways to discover malicious behavior through dynamic analysis, one is by executing the malicious behavior, the other

is by studying side-channels, e.g. "power consumption, electromagnetic emission, and timing analysis" [36].

Executing the malicious behavior could be practically impossible, as it could be programmed to execute only in very specific situations, such as after a long and specific list of operations. Attempting to find an arbitrarily long trigger like that is an exponential problem that quickly becomes computationally infeasible. Side channel attacks, on the other hand, requires a known-good chip for comparisons [36]. Under the assumption that these analyses are performed because the vendor is not trustworthy, it is not possible to verify anything as known-good if it is supplied by that same vendor.

7.2.5 ICT security

The previous section only focused on single components in an ICT system. ICT systems are made up of many parts, running a variety of software on a variety of hardware. This becomes a system of systems, consisting of many potentially vulnerable components.

> [V]erifying an ICT system to ensure that it is not doing harm is a monumental task. In principle, it entails a careful study of all the software components of several distributed systems running on top of each other. Each of these systems can easily consist of tens of thousands to hundreds of thousands of lines of program code. For each of the possibly hundreds of devices running the code that is involved in these distributed systems, we would have to study the operating system, device drivers, and hardware adaptation layers that run on them. The operating system itself can consist of tens of millions of lines of code. If it runs on a virtualized platform, we would also need to include the hypervisor in the study [40].

This monumental task does not even begin to address the issues related to hardware. In such complex and highly compound systems every component can conceivably contain hidden, malicious code. This is the kind off complexity that must be taken into account when establishing sufficiently critical system and securing it against external interference, regardless of whether this is done on the corporate or national level. This is no easy task, however, and Lysne concludes that "verifying the functionality of these components is not feasible given the current state of the art" [38].

Chapter 8

Discussion

The Internet has become ubiquitous in all aspects of modern life. This includes use in support of legitimate business, as well as in carrying out criminal activities. Despite the fact that misuse of computer systems is illegal under relevant national and international regulations, cyber operations have become an integral part of international politics. It is used for espionage, as a way to enforce national interests, and has become an alternative to conventional, physical attacks.

Computer misuse can take many forms, and be perpetrated by many different kinds of actors. In general terms all the forms of cyber attacks discussed in the previous chapters can be called cyber operations, in that they are operations carried out by an actor in the cyber domain, with a certain goal in mind. Moreover, because of the breadth of threat-actor types and the inherent problems with attribution of cyber operations it can often be hard to tell if an operation is carried out by a nation-state or some other actor. While the sophistication of an attack can give some indications of the capabilities of the threat actor, this is merely an indirect indicator, making it more likely for the attacker to remain anonymous following a cyber operation, than would be possible achieving the same goals using conventional means.

Because of this, the attribution problem also complicates the enforcement of the laws already in place to prevent cybercrime. If law enforcement is unable to attribute attacks to the attacker they are unable to enforce those laws. While these laws might not apply equally to cyber operations carried out by nation-states, there have been efforts to apply already existing international laws to the cyber domain, such as the Tallinn Manual [59], discussed in greater detail in Section 2.2. However, many nation-states do not seem to adhere to these attempts in the international cyber arena.

This refusal to acknowledge existing international regulation in the cyber domain, compounded by the difficulties of attributing a cyber operation to the true actor shows how laws are still not being fully enforced in cyberspace, insomuch that it can be difficult or impossible to hold any one actor responsible. In this relatively opaque environment, nation-states

can plausibly deny their own cyber operations and hypocritically accuse others. Furthermore, nation-states have shown a disregard for the effects which their cyber weapons can have on civilians. This has a number of consequences, as described next.

The most valuable form of cyber operations might be cyber collection. As long as we have had international politics a nation-state has had an interest in knowing what their neighbouring states are up to. OCEO, likewise, might seem like a logical translation of military operations or sabotage into the cyber domain. However, even if OCEOs are carried out with a specific target in mind, this does not mean that innocent third-parties are unaffected.

As shown above, the tools and weapons used for cyber collection and OCEO can leak, become publicly available and wreak havoc on organisations and civilians who were not intended targets. They can also possibly be reverse engineered by other nations or by advanced, non-governmental hacker groups, thereby proliferating in an uncontrolled manner. This appears to have become a regular occurrence, and as long as this happens as a result of cyberwarfare then it is unavoidable that innocent bystanders will come to harm due to collateral effects of the cyber operations. In a conventional war this would be unacceptable and break the very fundamental laws of war. This demonstrates the lack of regard that is given to the Tallinn Manual and its attempt at applying the rules of war to the cyber domain.

DCEO represents an interesting part of modern cyber operations. It seems, more than the other forms of cyber operations, to be purely a product of the cyber age. It also carries some important implications in how governments carry out cyber operations, and how these might be applicable to innocent third-parties.

One example of the sort of defensive measures carried out in a DCEO is *hack-backs*, i.e. retaliating by launching a cyber attack against the initial aggressor. Hack-backs have been a controversial practice for years. Both the legality and morality of the practice have been discussed, e.g. due to the uncertainties in attribution of cyber attacks. This controversy is spurred on by the fact that sophisticated attackers will carry out cyber operations several hops away from their physical position, e.g. from a botnet under their control, or from a server they have previously compromised. In this case the hack-backs might target the last hop used by the attacker, rather than their actual infrastructure. This can possibly end the attack, but might do so by disabling an innocent, third-party computer system.

The example of hack-backs illustrate that even when used only in the most, seemingly, benign way, i.e. only trying to stop an attack and not using retributive measures, DCEOs is still highly problematic as the target system might be owned by a third party. This third party might even be within the targets own borders, being exploited without their knowledge. While the

rules of war allow a state to defend itself from aggression, it is not free to harm its own citizens, or innocent parties in order to do so.

The relative lawlessness of the Internet, exemplified in the ways that nation-states carry out cyber operation with reckless abandon have had an enormous impact on the lives of regular people, and the day-to-day operations of many businesses. Cyber weapons on the loose are misused by criminals to extort the civilian populace with the power of the most advanced nation-states. Nation-state attacks against other nation-states have caused a direct financial loss for private businesses that are counted in billions of US dollars, and this does not even take into account the fact that USA keeps a literal kill-switch that could knock out power supplies to civilian hospitals, killing civilian as a direct consequence of their cyber operations.

There does not seem to be a lack of attempts to curtail dangerous cyber operations at the international level. USA and China have agreed that economic espionage is unwanted [45], the Paris Call attempted to have governments and businesses agree to oppose activity that could be harmful to the Internet [43], and experts in international law wrote the Tallinn Manual as a reference in how international laws and treaties can apply to the cyber domain. However many of the most advanced cyber nations did not sign the Paris Call, and the Tallinn Manual is an academic work that does not carry much significance in legislation.

Despite these potential barriers, many countries continue to carry out cyber operations. There is a regular stream of news stories wherein citizens, a company, a country's bureaucracy, or elected officials have been hacked. While this can clearly indicate criminal activity there have been too many incidents that show government involvement. Especially after the Snowden leaks it is hard not to recognize the involvement of the intelligence agencies and governments in these events.

When it comes to international relations and state interests they do as they please, with little or no regard for how their actions might affect third-parties. They will do their utmost to further their own agenda, even if this could potentially endanger civilians in their own country, or in the target country.

Moreover, for countries that do not have the same high regard of human rights, e.g. China, cyber capabilities offer new ways to surveil and exert control over the populace. The great firewall of China allows control of the accessibility to information. Mobile phones and technology like facial recognition make it possible to track the movement of citizens, and cyber operations make it possible to gain access to the most personal and private parts of a citizens life. Due to the low cost of entry for nation-states into the cyber domain, even small countries can implement such oppressive policies.

Even as most countries have laws against cyber crime and fraudulent

use of computer systems, for the reasons discussed throughout this thesis these laws are not sufficiently enforced when it comes to cyber operations across geographical borders. This has made the Internet, at best, a place where laws are only enforced in the rare cases where it is possible to trace the perpetrator. Alternatively, it has made the Internet a place where laws are not enforced, because they cannot be applied to the cyber domain, or simply because nation-states do not want to enforce them, thereby exploiting the relative lawlessness of the Internet.

This raises the question of how any organization can protect itself from these threats on the Internet? As discussed above there are many protective actions that can be taken. Building a strong defense in depth can be a large undertaking, however it is likely to be the best option to detect and prevent an attack from a sophisticated threat actor. We want to know whether such defenses can be built to stop even the strongest of nation-state threat actors.

This thesis has already shown how models such as the Cyber Kill Chain and the APT attack cycle can help in modelling and breaking down a sophisticated attack into separate components, that in turn can be analysed in order to create a timeline of any given attack. The models of the Pyramid of Pain and Detection Maturity Level have shown how defense in depth can not only improve defense, but actually turn one of the key strengths of an APT, its persistence, against itself in order to increase the pain of being discovered.

APTs and motivated nation-states have a rich repertoire of resources for executing cyber operations, from skilled personnel and advanced tools, to the knowledge of critical bugs and zero-day vulnerabilities. Bugs and vulnerabilities are an inherent and unavoidable part of modern software development, and as long as businesses need to run software with bugs and vulnerabilities, those bugs and vulnerabilities can be exploited by malicious actors.

The easiest and most reliable way to discover an attack is based on indicators collected from a previous attack. This inherently puts the defense at a disadvantage. While it is technically possible to investigate the capabilities of any piece of software or hardware ahead of implementation, these techniques can be extraordinarily cumbersome, to the point of being as good as impossible.

Ultimately, when faced with the full power, expertise, and financial weight of a nation-state, it is near impossible to set up an impenetrable defense, even for the biggest and strongest organisations. Even if the defender were able to do the monumental task of analysing every line of code, and every instruction handled by the computer before running it, a nation-state threat actor, maybe with the help of a vendor [30], may push a code update to circumvent security measures and introduce malicious code. Even if a company were able to fully analyse the full capabilities of a hardware chip, the act of analysing it also destroys it. There are

no guarantees that a shipment does not contain a limited amount of backdoored hardware [36].

This analysis shows that strong nation-state threat actors have at their disposal operation methods that it is practically impossible to defend against.

A consequence of this reasoning is that political alliances become extremely important in cyber warfare. In other words, it is important to be politically allied with nations that have strong cyber-operation capabilities. Then we are back to the traditional political landscape, where e.g. NATO becomes relevant for our national security, also in the digital domain.

Chapter 9

Conclusion

This thesis has analysed the current state of cyber warfare from several perspectives. In doing so it has attempted to give answer to some of the pressing issues in how nation-state cyber operations affect citizens and organizations.

With regard to Research Question 1 this thesis has shown how national and international laws are not properly enforced in cyberspace. This can happens because it is not possible, e.g. if trying to indict a foreign national performing cyber operations on behalf of their government. However, the lack of enforcement also stems from a complacent willingness to ignore the international laws regulating war, whenever it is in the cyber domain.

With regard to Research Question 2 this thesis has shown the lack of law enforcement in cyberspace impacts people and businesses, when advanced cyber weapons are leaked and repurposed by cyber criminals who turn them against civilians, or when cyber operations get out of hand and self-propagate across the Internet, where they might pose a severe risk to the health and safety of civilians.

With regard to Research Question 3 this thesis has shown how nation-states willingly abuse these circumstances to further their own agenda in cyberspace, this could be by performing economic espionage, or even turning their capabilities directly against their own populace, gradually eroding personal freedoms and the right to privacy.

With regard to Research Question 4 this thesis has shown how even the most mature organisations are helpless to defend themselves against a nation-state cyber operation. The complexity involved in verifying every piece of code is so high as to be practically impossible, especially when taking into consideration the facts that software would have to be continuously verified following updates. For hardware it is even worse, as any hardware analysed for these purposes would be destroyed, making it impossible to verify every single component.

Taken into consideration, this shows the fragility of society's reliance on the Internet as infrastructure. The ability to detect and mitigate cyber attacks have come a long way since the early days if the Internet, but it is still not mature enough to secure an organisation from a determined, strong, nation-state threat actor. As long as nation-state threat actors

continue to develop new ways of exploiting the inherent vulnerabilities in the fabric of the Internet, everyone will remain at risk of their cyber operations.

Bibliography

[1] S. Adee. "The Hunt For The Kill Switch." In: *IEEE Spectrum* 45.5 (May 2008), pp. 34–39. ISSN: 0018-9235. DOI: 10.1109/MSPEC.2008.4505310.

[2] S. D. Applegate and A. Stavrou. "Towards a Cyber Conflict Taxonomy." In: *2013 5th International Conference on Cyber Conflict (CYCON 2013)*. 2013 5th International Conference on Cyber Conflict (CYCON 2013). June 2013, pp. 1–18.

[3] William A. Arbaugh, William L. Fithen, and John McHugh. "Windows of vulnerability: A case study analysis." In: *Computer* 33.12 (2000), pp. 52–59.

[4] Associated Press. "US launched cyber attack on Iranian rockets and missiles – reports." In: *The Guardian* (June 23, 2019). ISSN: 0261-3077. URL: https://www.theguardian.com/world/2019/jun/23/us-launched-cyber-attack-on-iranian-rockets-and-missiles-reports (visited on 06/26/2019).

[5] James Ball, Julian Borger, and Glenn Greenwald. "Revealed: how US and UK spy agencies defeat internet privacy and security." In: *The Guardian* (Sept. 6, 2013). ISSN: 0261-3077. URL: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (visited on 04/30/2019).

[6] David Bianco. *The Pyramid of Pain*. Enterprise Detection & Response. 2013. URL: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html (visited on 03/07/2019).

[7] Leyla Bilge and Tudor Dumitraş. "Before We Knew It: An Empirical Study of Zero-day Attacks in the Real World." In: *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. CCS '12. New York, NY, USA: ACM, 2012, pp. 833–844. ISBN: 978-1-4503-1651-4. DOI: 10.1145/2382196.2382284.

[8] bk. *This activity is not APT10. It is all APT31 (or ZIRCONIUM) in our terms. The C2 domains that you mention were all registered and the threat actors made subsequent changes in specific ways that we attribute (with other information) to ZIRCONIUM.* @bkMSFT. Feb. 6, 2019. URL: https://twitter.com/bkMSFT/status/1093109336740642816 (visited on 02/11/2019).

[9] Jacob Børresen. *avskrekking*. In: *Store norske leksikon*. Sept. 20, 2017. URL: http://snl.no/avskrekking (visited on 06/21/2020).

[10] Siri Bromander, Audun Jøsang, and Martin Eian. "Semantic cyberthreat modelling." In: *CEUR Workshop Proceedings*. 11th International Conference on Semantic Technology for Intelligence, Defence, and Security (STIDS). Vol. 1788. Fairfax VA, USA: CEUR, 2016, pp. 74–78.

[11] Timothy Casey. "Threat agent library helps identify information security risks." In: *Intel White Paper* 2 (2007).

[12] Timothy Casey. "Understanding cyber threat motivations to improve defense." In: *Intel White Paper* (2015).

[13] Crowdstrike. *2019 CrowdStrike Global Threat Report*. 2019. URL: https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/ (visited on 04/17/2019).

[14] United States Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. DIANE Publishing, 2011. URL: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

[15] David Dittrich and Kenneth E Himma. "Active response to computer intrusions." In: *The Handbook of Information Security* 3 (2005).

[16] Mark Dowd, John McDonald, and Justin Schuh. *The art of software security assessment: Identifying and preventing software vulnerabilities*. Pearson Education, 2006.

[17] Philip Ewing. *If Mueller Report Was 'Tip Of The Iceberg,' What More Is Lurking Unseen?* NPR.org. 2019. URL: https://www.npr.org/2019/04/29/717594782/if-mueller-report-was-tip-of-the-iceberg-what-more-is-lurking-unseen (visited on 04/30/2019).

[18] Kevin Featherly. *ARPANET | Definition & History*. In: *Encyclopedia Britannica*. 2016. URL: https://www.britannica.com/topic/ARPANET (visited on 05/16/2019).

[19] Jim Finkle. "U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage." In: *Reuters* (2016). URL: https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108 (visited on 04/09/2019).

[20] FireEye. *Advanced Persistent Threat Groups*. FireEye. URL: https://www.fireeye.com/current-threats/apt-groups.html (visited on 05/15/2019).

[21] Angelyn Flowers and Sherali Zeadally. "US Policy on Active Cyber Defense." In: *Journal of Homeland Security and Emergency Management* 11.2 (2014), pp. 289–308. ISSN: 1547-7355. DOI: 10.1515/jhsem-2014-0021.

[22] Dan Goodin. *NSA-leaking Shadow Brokers just dumped its most damaging release yet*. Ars Technica. Apr. 14, 2017. URL: https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/ (visited on 05/15/2019).

[23] Andy Greenberg. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." In: *Wired* (2018). ISSN: 1059-1028. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (visited on 06/22/2020).

[24] Glenn Greenwald. "Glenn Greenwald: how the NSA tampers with US-made internet routers." In: *The Guardian* (May 12, 2014). ISSN: 0261-3077. URL: https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden (visited on 02/26/2019).

[25] Glenn Greenwald and Ewen MacAskill. "NSA Prism program taps in to user data of Apple, Google and others." In: *The Guardian* (June 7, 2013). ISSN: 0261-3077. URL: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (visited on 06/14/2019).

[26] Judah Ari Gross. *IDF says it thwarted Hamas cyber attack amid rocket barrage*. 2019. URL: https://www.timesofisrael.com/liveblog_entry/idf-says-it-thwarted-hamas-cyber-attack-amid-rocket-attacks/ (visited on 05/29/2019).

[27] Marte Halsør et al. *Granskarar: Kina hacka norsk selskap*. NRK. Feb. 6, 2019. URL: https://www.nrk.no/urix/granskarar_-kina-hacka-norsk-selskap-1.14418026 (visited on 02/07/2019).

[28] Eric M Hutchins, Michael J Cloppert, and Rohan M Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." In: *Leading Issues in Information Warfare & Security Research* 1.1 (2011), p. 80.

[29] Insikt Group. *APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign*. Recorded Future. Feb. 6, 2019. URL: https://www.recordedfuture.com/apt10-cyberespionage-campaign/ (visited on 02/11/2019).

[30] Audun Jøsang. "Potential cyber warfare capabilities of major technology vendors." In: *13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece*. 2014, p. 110.

[31] Jacob Kastrenakes. *Trump signs bill banning government use of Huawei and ZTE tech*. The Verge. Aug. 13, 2018. URL: https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump (visited on 05/28/2019).

[32] Paul Kocher et al. "Spectre Attacks: Exploiting Speculative Execution." In: *ArXiv e-prints* (Jan. 2018).

[33] Cyril Kowaliski. *Intel's Broadwell-U arrives aboard 15W, 28W mobile processors*. The Tech Report. 2015. URL: https://techreport.com/news/27557/intel-broadwell-u-arrives-aboard-15w-28w-mobile-processors (visited on 06/17/2019).

[34] Martin Lee et al. *Player 3 Has Entered the Game: Say Hello to 'WannaCry'*. 2017. URL: http://blog.talosintelligence.com/2017/05/wannacry.html (visited on 05/14/2019).

[35] Lockheed Martin Corporation. *Cyber Kill Chain®*. Lockheed Martin. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (visited on 06/04/2019).

[36] Olav Lysne. "Dynamic Detection Methods." In: *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?* Ed. by Olav Lysne. Simula SpringerBriefs on Computing. Cham: Springer International Publishing, 2018, pp. 67–74. ISBN: 978-3-319-74950-1. DOI: 10.1007/978-3-319-74950-1_8.

[37] Olav Lysne. "Reverse Engineering of Code." In: *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?* Ed. by Olav Lysne. Simula SpringerBriefs on Computing. Cham: Springer International Publishing, 2018, pp. 47–55. ISBN: 978-3-319-74950-1. DOI: 10.1007/978-3-319-74950-1_6.

[38] Olav Lysne. "Summary and Way Forward." In: *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?* Ed. by Olav Lysne. Simula SpringerBriefs on Computing. Cham: Springer International Publishing, 2018, pp. 109–116. ISBN: 978-3-319-74950-1. DOI: 10.1007/978-3-319-74950-1_12.

[39] Olav Lysne. *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust Into Electronic Equipment?* Vol. 4. Springer, 2018.

[40] Olav Lysne. "What Is an ICT System?" In: *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?* Ed. by Olav Lysne. Simula SpringerBriefs on Computing. Cham: Springer International Publishing, 2018, pp. 21–30. ISBN: 978-3-319-74950-1. DOI: 10.1007/978-3-319-74950-1_3.

[41] Mandiant Intelligence Center. *APT1: Exposing one of China's cyber espionage units*. 2013, p. 76. URL: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[42] Jenna McLaughlin. "Apple Slams Order to Hack a Killer's iPhone, Inflaming Encryption Debate." In: *The Intercept* (Feb. 17, 2016). URL: https://theintercept.com/2016/02/17/apple-slams-order-to-hack-a-killers-iphone-inflaming-encryption-debate/ (visited on 06/14/2019).

[43] Ministère de l'Europe et des Affaires étrangères. *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*. France Diplomatie :: Ministry for Europe and Foreign Affairs. URL: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in (visited on 01/29/2019).

[44] Henrik Moltke. *Mission Creep: How the NSA's Game-Changing Targeting System Built for Iraq and Afghanistan Ended Up on the Mexican Border*. The Intercept. May 29, 2019. URL: https://theintercept.com/2019/05/29/nsa-data-afghanistan-iraq-mexico-border/ (visited on 05/31/2019).

[45] Ellen Nakashima and Steven Mufson. *U.S., China vow not to engage in economic cyberespionage*. Washington Post. 2015. URL: https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html (visited on 01/29/2019).

[46] Ellen Nakashima and Joby Warrick. *Stuxnet was work of U.S. and Israeli experts, officials say*. Washington Post. 2012. URL: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (visited on 04/09/2019).

[47] NATO. *Cyber Defence Pledge*. NATO. 2016. URL: http://www.nato.int/cps/en/natohq/official_texts_133177.htm (visited on 04/19/2019).

[48] Barack Obama. *Presidential policy directive/PPD-20*. Washington: White House, 2012.

[49] Pierluigi Paganini. *Equation Group APT and TAO NSA: Two Hacking Arsenals Too Similar*. InfoSec Resources. Mar. 9, 2015. URL: https://resources.infosecinstitute.com/equation-group-apt-tao-nsa-two-hacking-arsenals-similar/ (visited on 02/26/2019).

[50] Lewis Page. *Israeli sky-hack switched off Syrian radars countrywide*. 2007. URL: https://www.theregister.co.uk/2007/11/22/israel_air_raid_syria_hack_network_vuln_intrusion/ (visited on 05/29/2019).

[51] Jose Pagliery. "Iran hacked an American casino, U.S. says." In: *CNN* (Feb. 27, 2015). URL: https://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html (visited on 06/27/2019).

[52] Paris Call. *Supporters — Paris Call*. URL: https://pariscall.international/en/supporters (visited on 06/24/2020).

[53] Jordan Pearson. *These So-Called 'ISIS Kill Lists' Are a Great Reminder to Change Your Password*. Vice. June 16, 2016. URL: https://www.vice.com/en_us/article/qkj3j3/these-so-called-isis-kill-lists-are-a-great-reminder-to-change-your-password (visited on 05/07/2019).

[54] Tom Phillips. "Edward Snowden claims US hacks Chinese targets." In: (2013). ISSN: 0307-1235. URL: https://www.telegraph.co.uk/news/worldnews/northamerica/usa/10117478/Edward-Snowden-claims-US-hacks-Chinese-targets.html (visited on 01/09/2019).

[55] Quartz. "What you need to know about China's intelligence law that takes effect today." In: *Quartz* (2017). URL: https://qz.com/1016531/what-you-need-to-know-about-chinas-intelligence-law-that-takes-effect-today/ (visited on 05/28/2019).

[56] Michael Safi. "Isis 'hacking division' releases details of 1,400 Americans and urges attacks." In: *The Guardian* (Aug. 13, 2015). ISSN: 0261-3077. URL: https://www.theguardian.com/world/2015/aug/13/isis-hacking-division-releases-details-of-1400-americans-and-urges-attacks (visited on 05/07/2019).

[57] David E. Sanger. "Utilities Cautioned About Potential for a Cyberattack." In: *The New York Times* (Feb. 29, 2016). ISSN: 0362-4331. URL: https://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html (visited on 06/27/2019).

[58] David E. Sanger and Nicole Perlroth. "U.S. Escalates Online Attacks on Russia's Power Grid." In: *The New York Times* (June 15, 2019). ISSN: 0362-4331. URL: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html (visited on 06/23/2020).

[59] Michael N Schmitt. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.

[60] Michael N. Schmitt. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Feb. 2017. DOI: 10.1017/9781316822524.

[61] Mark Seaborn and Thomas Dullien. *Project Zero: Exploiting the DRAM rowhammer bug to gain kernel privileges*. Project Zero. Mar. 9, 2015. URL: https://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html (visited on 06/03/2019).

[62] Catherine Shu. *Australia bans Huawei and ZTE from supplying technology for its 5G network*. TechCrunch. 2018. URL: http://social.techcrunch.com/2018/08/22/australia-bans-huawei-and-zte-from-supplying-technology-for-its-5g-network/ (visited on 05/28/2019).

[63] Øyvind Bye Skille. *Tvil om hvem som står bak Visma-hackingen*. NRK. Feb. 8, 2019. URL: https://www.nrk.no/norge/tvil-om-hvem-som-star-bak-visma-hackingen-1.14420262 (visited on 04/16/2019).

[64] Ryan Stillions. *The DML model*. Ryan Stillions: Postulations after great cogitation. 2014. URL: http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html (visited on 02/11/2019).

[65] Jens Stoltenberg. *NATO Will Defend Itself (Article by NATO Secretary General Jens Stoltenberg Published in Prospect)*. NATO. Aug. 29, 2019. URL: http://www.nato.int/cps/en/natohq/news_168435.htm (visited on 06/09/2020).

[66] Ellery C Stowell. "Convention relative to the opening of hostilities." In: *American Journal of International Law* 2.1 (1908), pp. 85–90.

[67] Symantec Corporation. *Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak | Symantec Blogs*. 2019. URL: https://www.symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit (visited on 05/15/2019).

[68] *The Geneva Conventions of August 12, 1949*. Geneva: International Committee of the Red Cross.

[69] Trend Micro. *Hacktivism 101: A Brief History and Timeline of Notable Incidents - Security News - Trend Micro USA*. 2015. URL: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/hacktivism-101-a-brief-history-of-notable-incidents (visited on 04/08/2019).

[70] Jo Van Bulck et al. "Foreshadow: Extracting the keys to the intel SGX kingdom with transient out-of-order execution." In: *27th USENIX Security Symposium (USENIX Security 18)*. 2018, pp. 991–1008.

[71] Steven J. Vaughan-Nichols. *The day computer security turned real: The Morris Worm turns 30*. ZDNet. 2018. URL: https://www.zdnet.com/article/the-day-computer-security-turned-real-the-morris-worm-turns-30/ (visited on 03/13/2019).

[72] Zack Whittaker. *Iran behind bank cyberattacks, U.S. government officials say*. ZDNet. 2013. URL: https://www.zdnet.com/article/iran-behind-bank-cyberattacks-u-s-government-officials-say/ (visited on 01/09/2019).

[73] Kim Zetter. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." In: *Wired* (Nov. 3, 2014). ISSN: 1059-1028. URL: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (visited on 12/03/2018).

[74] Kim Zetter. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." In: *Wired* (July 11, 2011). ISSN: 1059-1028. URL: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ (visited on 05/14/2019).

.