Strategies for Malware in Cyber Conflicts

Vanessa Robl
Supervisor: Dr. Heiko Niedermayer
Seminar Future Internet SS2017
Chair of Network Architectures and Services
TUM Department of Informatics, Technical University of Munich
E-Mail: robl@in.tum.de

ABSTRACT

Over the course of the past few decades, the advancement of technology went farther and farther, reaching into nearly every corner of our lives. Information, or the deliberate concealment of it, can have an immense impact on the outcome of a volatile situation. Especially with regard to warfare the global interconnectivity of business, government, and infrastructure combined with a dependence on IT systems in all aspects of society brought forth a multitude of application possibilities which have never existed before. Conflicts can now partly be fought behind a computer screen. Lacking technological progress or the effort of highly skilled individuals can turn tables, providing major advantages or disadvantages to either participating side. In this paper, the term Cyber Conflict in association with Advanced Persistent Threats will be discussed. Thereby, the focus will lie on tools and strategies that are commonly used, as well as on methods on how to detect, defend from or distribute exploits.

Keywords

Cyber Conflict, Advanced Persistent Threats, Exploits

1. INTRODUCTION

"Cyber attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security."[1]

With the introduction of personal computers to homes and businesses in the 1970s, the foundation was laid for the development of the enormous global network of interconnected autonomous networks we know today as the Internet. It became a tool offering great opportunities, but at the same time it came with a vast amount of risks. Where there were people to strive for education, knowledge or an open market there were also those to operate for their personal gain, gathering information, finding loop holes, dismantling organized structures. In general, networks have grown unbelievably large. Most command and control systems are connected to the Global Information Grid (GIG) or have embedded chips, making them vulnerable. The bigger the network, the higher the risk for a successful intrusion since it is harder to cover up such a huge attack surface. Additionally, the more influential or valuable the data within the system, the higher the temptation to sneak in and steal the data. Although the technological advance brought with it enormous and radical changes and benefits to our society it, at the same time, entails more and more risks.

To name only a few threats, there is malicious software like Trojans, Viruses, and Worms which can infect a computer system as well as Denial of Service attacks or Phishing. All of them have more or less the same goal to compromise the target system and benefit the attacker. The victims of such attacks are regular users as well as companies or even governments.[1][2]

Within this work, we will have a look at the agendas both attackers and defenders have as well as at strategies and tools that are used to achieve those.

2. DEFINITION AND TERMS

Before we can dive into the analysis of strategies regarding attack and defense of system vulnerabilities, we first need to establish some terms and definitions that will be used in the scope of this work.

2.1 Cyber Conflict[3]

Cyber Conflict or Cyber Warfare is a term defined as *"a tense situation between and/or among nation-states and/or organized groups where unwelcome cyber attacks result in retaliation."*[4] Involved are two or more opposing parties which can be made up of state-actors, companies, criminal organizations, hacktivists or similar. Strategies include defense against incoming attacks on infrastructure, economic disruption or loss of vital information while at the same time attacking the opponent in the hopes of causing damage, spreading confusion, using obfuscation to cloud movements or gaining valuable knowledge.

Cyberwar and conventional warfare in itself arenâĂŹt that different, both use the same means to achieve a strategic objective: attacking and espionage. Attacks are aimed to cause immediate damage or disruption to vital points within the enemies area of operation while espionage is a used to gaining an advantage by knowing more about the enemy than vice versa. Strategies and goals in both are quite similar as well when looking at the big picture. Despite these similarities, there is one glaring difference: the low barrier of entry. Cyber weapons are cheap and do not require significant infrastructure, financing or physical space for development and assembly. To deliver a potentially devastating attack on a city or even a whole country, the only tools needed are a computer, an Internet connection, and knowledge. In addi-

doi: 10.2313/NET-2017-09-1_10

tion, detecting or defending against a cyber weapon can be extremely difficult.

2.2 Advanced Persistent Threat[5]

Advanced Persistent Threats (APTs) are a special type of sophisticated and well-planned attack on a computer system, compromising it stealthily with the goal of staying undetected for as long as possible while continuously sending gathered data back to the attacker. Generally it can be organized into six successive phases:

Phase 1: Reconnaissance & Weaponization

- information about target is collected
- vulnerabilities are identified
- multiple attack patterns are prepared to be able to adapt to different cases

Phase 2: Delivery

- delivery of the exploit via the identified vulnerability
- direct delivery: attackers send exploits directly via various techniques (e.g. malicious email, drive-by downloads)
- indirect delivery: a trusted third party is compromised and the exploit is implanted by using them

Phase 3: Initial Intrusion

- exploit is successfully executed
- typically, backdoor malware is installed, granting access to the attacked system
- also possible: login credentials of the target have been obtained
- goal: establish a foothold in the compromised network

Phase 4: Command & Control

- taking control of the target network
- enabling further exploitation
- evading detection through the use of various methods for obfuscation

Phase 5: Lateral Movement

- discovering and collecting data
- internal mapping of the network
- taking control of additional (neighboring) systems
- usually longest lasting phase
- goal: getting large amounts of data over longest amount of time while running low to avoid detection

Phase 6: Data Exfiltration

- extracting the gathered data securely from the target system to a neutral system
- often: compression and encryption of the data
- hiding transmission

APTs are key tools in serious cyber conflicts. They are complex, tailored very carefully onto a specific target which has been chosen regarding its tactical and informational value. A high amount of skill, knowledge, and time is needed, but the gain in case the attack is successful can be tremendous. In a conflict, it is they ideal weapon, offering the possibility of high impact while having anonymity, thus, making it a dangerous and serious threat. For that reason, we will take a closer look at APTs in the scope of this work.
This paper will focus on the strategies and tools used in Phase 3: Initial Intrusion and Phase 5: Lateral Movement.

2.3 Exploits[6][7]

An exploit is a program specialized on taking advantage of weaknesses and vulnerabilities in auxiliary or application programs to gain access to systems and compromise them with the goal of obtaining advanced privileges like administrator rights.
There are various kinds of exploits, for example:

- **Local exploits:** can be activated by opening seemingly harmless files if the program with which it is opened has been compromised using a security flaw within it
- **Remote exploits:** an attack using manipulated data packets or specific bitstreams on weak spots in the network software
- **DoS exploits:** purposefully overload an application until it stops working
- **Zero day exploits:** term used for an attack using a yet undetected security loophole, making the developer aware of the vulnerability once he notices the intrusion

Protection from exploits starts with the careful programming of applications with the goal of having close to zero vulnerabilities. In addition, intrusion detection systems and intrusion prevention systems can help in finding and maybe even intercepting incoming attacks.

2.4 Persistence and Stealth[8]

Stealth and persistence are terms that will be used in a very specific way in the following context:
"The Stealth of a resource is the probability that if you use it now it will still be usable in the next time period. The Persistence of a resource is the probability that if you refrain

doi: 10.2313/NET-2017-09-1_10

from using it now, it will still be usable in the next time period."[8]
Stealth is designed to evade detection during transit, execution or when a program is at rest, whereas persistence is drafted to stay within an affected system or network beyond the termination of the delivery mechanism that was used.
High-level Advanced Persistent Threats are modeled in a way as to maximize the value of these afore-mentioned resources. The act of balancing the two factors to reach that maximum is a challenging task involving deep knowledge, calculation, and foresight to be able to assess the optimal time to strike. Thereby, the stakes and gains have to be taken into consideration. These values can not be calculated accurately or with certainty, since one can only assume what the situation, for example between two competing nation-states, might be in the future.
Formally, stealth and persistence can be depcited as equations (taken from Ref. [8]):

$$Stealth = Pr(resource\ survives|use\ it) \quad (1)$$

$$Persistence = Pr(resource\ survives|not\ use\ it) \quad (2)$$

Benchmarks for stealth and persistence are, for example, that the average duration of an attack based on a zero-day-exploit is 312 days (stealth) and that only three to five percent of vulnerabilities in popular browsers could be rediscovered within a three-years period (persistence). Both variables, of course, are also dependent on the state of the target system. Against a defender that keeps his system up-to-date and is overall well-protected, the stealth and persistence values will be lower than against one who is more lenient. Overall, the best time to strike is, when the gain is high enough to counterbalance the risk involved.

3. GOALS IN CYBER CONFLICT

In today's world a large amount of critical areas depend on large networks, partly using the Internet excessively: agriculture and food, banking and finance, communication, critical manufacturing, emergency services, energy, healthcare, nuclear reactors, transportation systems, and water to name just a few. A successful attack on any of these could potentially have disastrous consequences.[2]
There can be various motivations for an attack (taken from Ref. [12]):

- **Political:** protest against political action; protest against laws or public documents; protest against acts related to physical violence; espionage
- **Economical:** personal or corporate financial greed; espionage
- **Socio-cultural:** competition between groups over diverging goals, scarce resources; ethnic conflict

Being successful in a cyber conflict depends on two things: means and vulnerability. That means, the outcome is heavily influenced by the people, tools, and cyber weapons (means) available to each side and by the the extent to which either party uses the Internet and networks within their economy and military (vulnerability). The overall goal is to have higher educated employees than the enemy equipped with a more extensive and sophisticated set of tools and carefully developed cyber weaponry. This, of course, is only efficient if the enemy country is at a state of development where an attack directed towards networks will have an actual impact. For example, it would not make sense to order an attack on water and electricity distribution facilities aimed at a rural village with no water supply lines or electrical lead. Too big of a difference in technological development can make the use of cyber attacks obsolete.[13]
So far we looked at overall sources of motivation and general goals. For software or tools, there exist different kinds of goals depending on the purpose and the desired effect which can roughly be divided into Stealth and Persistence and Maximum Damage.
Majorly used in espionage, Stealth and Persistence based attacks aim at quietly infiltrating a system and staying there undetected as long as possible but with a reasonably well-established access to valuable data or essential settings. The goal, thereby, is, of course, to gather a large amount of usable information or to manipulate the system gradually and stealthily, reutilizing the same routine again and again. APTs can be classified as Stealth and Persistence attacks.
A variation of that which uses both aspects, Stealth and Perception as well as Maximum Damage, is planting a program into a system to disrupt or destroy it effectively at the optimal moment. This includes staying undetected until the attacker decides to start it. The more time passes, the higher the risk that either the malicious program itself or the attackers backdoor access for triggering it will be found. Also, if the attacking party miscalculates, and launches it either too early or too late, the desired effect might have way less impact or none at all.
For the Maximum Damage approach it is not necessarily important if the used tool or weapon can not be reutilized in other attacks, be it because it was detected and made public or because after detection there were countermeasures taken to prevent a similar or the same attack. After successful intrusion, the used tool will try to do the highest amount of damage possible without regards to stealth or persistence.
In comparison to attacking, when being hit by an attack or intrusion, the system recovery often is the top priority. By doing that, evidence necessary to determine how the systems was compromised is lost. Thus, the goal for a defending party is to do forensic work before a reload or it will be impossible to determine where the attack came from and how to develop countermeasures to prevent it from happening again. Generally, of course, the goal for a defending party is to prevent any kind of attack from happening in the first place by having strict security standards in place.[2]

4. TOOLS FOR CYBER CONFLICT

With the advance in technology it became impossible to rely solely on ones own skill in programming to mount a successful attack. There's a variety of tools available which are not necessarily meant for this abuse but, nevertheless, serve a much-needed purpose in aiding offenders. They can be categorized as follows:

- Reconnaissance tools
- Scanning tools

doi: 10.2313/NET-2017-09-1_10

- Access and escalation tools
- Sustainment tools
- Obfuscation tools
- Exfiltration tools
- Assault tools

A large amount of these applications are open source and/or freeware and are developed further and kept up-to-date constantly. In the following, we are going to look at each of the listed varieties, although we will mainly focus on those that might be useful for the before-mentioned APT-phases 3 and 5: Initial Intrusion and Lateral Movement. Every category will have the respective phase in brackets.[2][9][10]

Reconnaissance tools (Phase 1)
Reconnaissance Tools are used to gather information by, for example, accessing public websites, looking up Domain Name Server (DNS) records or collecting metadata from documents. For that, one can use automated data mining or search engines to filter for certain keywords. There are some search engines that can retrieve information even from the so-called "Deep Web" which normally is not accessed by the standard search engine.
An exemplary tool to find out information about domain names all over the world is textitWhois. It returns contact information which, in addition to the name server, may include the physical address, phone number, and contact name from someone linked to the domain if they are not hidden by a proxy. There is also the possibility to run a query for the actual IP address in case it is already known. If not, given the name server, one can use the command line queries *nslookup* or *dig* (list of all dns entries in a certain domain) to retrieve it. With this basic information plus perhaps additional auxiliary tools, it is possible to dig deeper and gather even more information.
Another approach on getting to know more about the target system is the use of metadata. Metadata is, so to speak, data about data. Looking at a regular file this might be, for example, user names who edited the file, paths where the file has been stored, coordinates of where a certain picture was taken, image thumbnails, and many more. Applications that aid users in finding this information are, among others, *Metagoofil* and *Exiftool*.
The best defense against tools such as those is to restrict as many sources of information as reasonably possible. Regarding the DNS server, one can deny zone transfer to unknown machines or use proxies to replace the actual data. Removing metadata can be done using the same tools as mentioned above. Of course, there will always be a certain amount of data that can't be hidden away completely, but limiting that amount is a first step to make a system more secure.[2][9][10]

Scanning tools (Phase 1)
The purpose of scanning tools is to find information about the system environment and the system itself in detail. They are positioned in a way to either have direct network access, or to be able to listen to network traffic, especially if the target system is connected to the Internet. Scanners, for example, try to map networks, scan ports, and determine the operating system a target host is running on.
Applications like *Nmap* and *Nessus* can be used to ping IPs, detect vulnerabilities, fingerprint operating systems, run traceroutes, scan ports, and much more. Some features involve detection avoidance, changing the speed of processes, and changing the communication method.
To defend a system from such tools is difficult. For the scanners to not pick up any information, there has to be no detectable data leakage at all. Traffic should always be encrypted and the usage of standard ports (like port 22 for SSH) should be avoided. Proper implementation of firewalls and the use of reverse proxies which limit the number of exposed ports and are meant to obfuscate the underlying system as well as analyze incoming requests can help as well.[2][9][10]

Access and escalation tools (Phase 3 to 5)
Access and escalation tools, as the name suggests, focus on gaining access to a system and, then, taking control of it and trying to expand this control. For this, a vast variety of applications is available. Some of the most commonly used ones are: *Hydra*, *John the Ripper*, *Metasploit*, and *Canvas*.
Both *Hydra* and *John the Ripper* are password attackers. They aim to find a working username and password combination for a target system, eg a webpage or a database, to gain easy access. While *Hydra* works through lists of possible passwords, similar to a limited brute-force-attack, *John the Ripper* attempts to recover the original password from an acquired hash.
In contrast to the afore-mentioned, rather basic, attack tools, the *Metasploit Project* operates in a more advanced fashion. It effectively aids an attacker in using exploits to invade a system. With a built-in list of usable bugs and exploits it checks if the target system is vulnerable to any of them and hands the user a selection of possibilities. The chosen method together with a configured payload that will be executed on the target system is encoded and, then, executed. Thereby, it is indispensable to have a certain degree of knowledge about the target which can be obtained by using one of the above-mentioned Reconnaissance or scanning tools. Similar to *Metasploit*, *Canvas* is based on using a library of exploits and payloads to compromise a system as well. Although its library is not quite as extensive as others, it is updated far more regularly, keeping up with the fast moving changes in the cyber environment.
A password policy with strong passwords and regular changes as well as patching and system hardening can keep tools such as this at bay to a certain extent. In regards to passwords: They should be at least 8 digits long, have at least one number and one symbol, and should contain both uppercase and lowercase letters. In addition, they should be changed around every three months. To defend against exploit abuses, one should always patch and update the system as fast as possible. In addition, it is beneficial to disable all ports, services, accounts, etc that are not absolutely necessary for the system to function. Taking these steps already has a great impact on the possible ways an attacker can gain access.[2][9][10]

Sustainment tools (Phase 3)
Once the desired level of infiltration has been reached after the first breach, an attacker needs to make sure that he can continue accessing the system since it may very well be possible that the vulnerability that has been used will be fixed

by a patch or similar measures in the future.
The easiest and, at times, most effective way to ensure that, is to create an account with the necessary rights for ones own use. This can be accomplished by simple system commands such as *useradd* or *netuser*. Nevertheless, there are better and less detectable methods, for example, installing a backdoor. A programmer with enough background knowledge can easily write such code by himself, but there is also a list of web-based methods found in the *Web Backdoor Compilation*. Additionally, for those who do not want to program themselves, there is a tool available called *Netcat* which will create a listening port granting access to a shell on the system. Using some tweaks, tactical renaming of the tool, and the careful selection of the used ports can minimize the risk of detection.
The defense against such actions can be divided into two parts. Firstly, by hardening the system as best as possible and restricting incoming and outgoing traffic we can make the insertion of backdoors difficult from the start. In addition, with the help of applications such as *powerbroker* or *Cisco Security Agent (CSA)* one can lock down administrative access to the system as a preventive measure against unwanted installations. Secondly, close monitoring of accounts, system accesses, open ports, and similar instances can help finding already installed backdoors. Since this is an immensely time-consuming task, most will not observe their system in such a way, thus, well-hidden installations may never be found.[2][9][10]

Obfuscation tools (Phase 4 and 5)
In order to stay hidden and undetected while covering their tracks at the same time, attackers need obfuscation tools. Generally, there are three main concerns.
Firstly, both the logical and physical location needs to be obscured. To do that, the use of proxies is common. Tools such as *The Onion Router (TOR)*, *Bitblinder* or *Perfect Dark* provide this service, offering anonymity of communication. Similarly, Virtual Private Networks (VPNs) or compromised private systems can be utilized as manual proxy.
Secondly, it is important for an attacker to eliminate all log files generated by his actions within the network to cover his tracks from future investigations or system administrators. With administration rights, most logs can easily be manipulated using simple text editors. If that approach fails, one can try to erase them entirely or overwrite them with self-generated events. In the worst case, if detection has to be avoided at all costs, extreme measures such as the use of assault tools to destroy or disrupt the system entirely have to be taken.
Thirdly, in case an intruder changed or created files and wants to hide those, there are different kinds of approaches. For example, one can rename the files and hide them within a list of similarly named files or use tools like *slacker* to hide them in places which are not easily accessible to users. With the help of the *NTFS file system* it is even possible to place data in Alternate Data Streams (ADS), storage areas originally intended for metadata. One more thing that has to be taken into account is to adapt the timestamp, so that it won't stand out from regular files. They are easily manipulated by either simple command line queries or a tool like *Timestomp*.
Defense against obfuscation tactics is almost entirely based on reaction instead of prevention. Without enormous resources or tactically placed layers it is very difficult to backtrack activities to the original location if the proxy is set up sufficiently. In certain cases, the application of tools that specialize in root kit detection can be helpful regarding preemptive measures. In contrast to that, defending against file and log manipulation is a bit easier. There are many measures that can be put in place, for example utilizing a tool called *Tripwire* to monitor for changes in realtime and alerting the defender when something seems out of place. Securing log files can be done by regularly storing them on a remote server, making them difficult to reach.[2][9][10]

Exfiltration tools (Phase 6)
After compromising a system and gathering data, it's necessary to have some way of retrieving all this information and putting it somewhere safe and more easily accessible. For that, exfiltration tools are needed. This can involve either physically transporting the data, using unfiltered protocols or hiding it through encryption.
For physical exfiltration, any storage media (memory card, USB stick, etc) can be used. With the progress in technology resulting in more and more disk space on smaller and smaller devices transporting them undetected is getting easy.
Another way to hide data effectively would be the use of encryption or steganography tools such as *TrueCrypt*, *Puff* or *OutGuess*. With them, collected information can be hidden from or at least made unreadable for a third party.
A third option could be to use the protocols that are already in place. It is, for example, possible, to send the encrypted and fragmented data via email. As an alternative, one can also use tools such as *OzymanDNS* to transmit the information via various protocols, such as HTTP or DHCP.
Unless the environment in which the system is located is restricted and diligently monitored or Data Loss Prevention (DLP) tools are used, it is extremely difficult to prevent anyone from exfiltrating data.[2][9][10]

Assault tools
Assault tools can not be assigned to an APT phase since the intention of APTs is to stay undetected for a long period of time while stealing data continuously instead of causing damage to the system. Nevertheless, they are an important part of Cyber Conflict. There is a vast amount of tools and methods available to harm, manipulate or temporarily disable a target. They can be related to both, software and hardware.
Once an attacker has administrative rights on a system, it is extremely difficult to prevent him from intercepting the regular workflow. Thus, the only effective way to defend against such an assault is to prevent attackers from gaining administration privileges in the first place. In some cases, there are users with admin rights who only need them for a limited amount of applications. Here, restricting the rights and assigning them solely for the purpose of executing those programs can secure the system further.
Affecting the software can, for example, be done by tampering with the system resources. Although easily detectable, it is a foolproof way to disturb a system. Using simple commands to fill up free space on the disk is only one way to make a computer unusable. Resources such as memory, CPU, and hard disk can be abused to run the attackers own implanted process, thus, preventing regular processes from working correctly. A less obvious, but also destruc-

doi: 10.2313/NET-2017-09-1_10

tive method involves the deliberate manipulation of the system environment. Many applications which depend on very specific settings can become unusable if one makes small changes. One of these delicate variables is time since a huge amount of programs depend on this variable to be consistent and correct over an extended period of time. There are various other small changes that can be made with an equally destructive result.
Methods to attack the hardware are generally a bit more complex. One way could be to rewrite Read Only Memory (ROM) modules which often contain firmware regulating how certain pieces of hardware function or communicate with each other. An easier way of attacking would be to tamper with the driver files, thereby, directly messing with the software that communicates with the hardware. This is only a temporary disruption, though, since it works only until the affected driver is reinstalled. There are many ways for attacking the hardware, but one of the most significant ones would be to interfere with the Supervisory Control and Data Acquisition (SCADA) system.[2][9][10]

To secure a system in general, there are various standard tools that should be used in a preventive measure such as firewalls, real time anti-virus protection, anti root kits, monitor tools, code review tools, and many more. Without basic protective programs, users basically open the doors to attacks on their systems. Of course, using such tools for defense doesn't give one hundred percent security, but by regularly scanning the system for programs with unusual behaviour or warning the user when an unauthorized download is happening, for example, can filter out at least some of the threats.

Attacking and defending with tools in a real cyber conflict can look like like the following:
In September 1998 the Electronic Disturbance Theater (EDT) attacked the Pentagon, trying to achieve a Denial-of-Service. Thereby, EDT developed malicious code and browser addins that reloaded a page over and over, resulting in a shutdown of services if enough people gather on the same target website (now known as *FloodNet* software). The defenders, as a response, programmed their websites in a way that, if a *FloodNet* attack was detected, the site would open a new window with every reload, eventually overloading the attacking system, causing it to shut-down and, thus, preventing the attack.[11]

5. STRATEGIES USED IN CYBER CONFLICT

Strategy as defined in Ref. [14] is the act of *"managing context for continuing advantage according to policy"* building on a systematic combination of goals and objectives, resources and capabilities, and ways to accomplish these goals and objectives.

5.1 Attack Strategies

Given the current stage of technology a strategic cyber attack by itself is not likely to be decisive for war. With a possibly uncontrollable blowback effect, parties involved in a conflict run a high risk of being hit back with the same attack they launched or with another, similarly disruptive one, unless the level of advancement in technology is vastly different. Generally though, the states that are most likely to develop the technological know-how on how to create and use a cyber weapon are also the most dependent on their own network infrastructure. Therefore, instead of launching direct attacks, using cyberwarfare capabilities on an operational level, as aid for regular troop movement and war strategy, might be more feasible. Nevertheless, cyber weapons can not, with some rare exceptions, destroy actual equipment permanently. The damage it can do is to confuse or interfere, to disable systems temporarily or to delay and obstruct certain processes.[13]
Based on this observation, reasonable objectives for a strategic cyber attack can be espionage, propaganda, Denial-of-Service (DoS), data modification or infrastructure manipulation.

Espionage
Cyber espionage is an expansion of the traditional effort to collect information on the enemies secrets, intentions, and capabilities. This includes the search for classified, personal or corporate data, intellectual property, proprietary information and patents as well as results from research and development projects. The gain in targeting sensitive information can possibly be very high. Stealing data can be done anonymously and remotely from all over the world which makes it a great strategic tool.[13][15]

Propaganda
Strategically placed propaganda can have a huge impact on peoples awareness and opinion on certain facts or situations. Using the amplification power of the Internet where digital data can be copied and sent instantly, a message can be spread within a short amount of time anywhere in the world. Casting doubt or spreading fear can have a huge impact on the pressure a government is exposed to, possibly even forcing it to behave differently to ensure the peoples support.[15]

Denial-of-Service
DoS is commonly used to temporarily make certain services or systems unavailable by flooding it with data or requests until it is unable to process all the data and simply shuts down. Other variations include the physical destruction of hardware or the use of electromagnetic interference which destroys unprotected electronics via current or voltage surges. From this, various strategical advantages can be gained. Depending on the targeted system and its use, there could be a loss of communication, a permanent loss of data, temporary blindness regarding surveillance or movements, loss of control over remotely controlled entities, and many more.[13][15]

Data modification
Corrupting data with a stealthy and undetected cyber attack can result in critical errors or wrong decisions made by the enemy based on their trust in the integrity of the information stored in their own network. Data modification can vary from implanting ones own propaganda or misinformation in a neutral or adverse website to the compromising of advanced weapons or command-and-control systems.[2][15]

Infrastructure manipulation
As mentioned before, the technological advances have given birth to highly vulnerable critical infrastructure connected to the Internet but without proper protection due to insuf-

doi: 10.2313/NET-2017-09-1_10

ficient computing resources or hardware restrictions. Some are dependent on realtime or automatic responses, making it more difficult to replace a failing systems with a human. A successful strike against, for example, an electricity plant or the traffic light system could lead to severe repercussions.[15]

Even though cyber attacks are not as obviously destructive as, for example, a bomb, when used correctly they can make a huge difference and give strategical advantages. In a conflict with more or less equipollent sides, it can turn the scale.

5.2 Defense mechanisms

Building up a decent and solid defense against attackers is a strategic challenge as technology and new software is developed so quickly that it is impossible for any organization to keep up-to-date with all of them. It is simply have too much ground to cover. An attacker only has to succeed once, whereas a defender has to constantly search for loopholes and improve, update, and maintain the overall system. In addition, it has to be guarded against insider threats and mobile devices that migrate in and out of the work environment.[2][15]
Nevertheless, defenders can make the most out of their situation. They have the 'home-field advantage' and with administration rights throughout the network they can change hardware and software configurations to their liking making their system unique and, thus, harder to crack since the standard vulnerabilities may not be there anymore. Knowledge is key. If a defender can limit the amount of information a reconnaissance or scanner tool can gather, it is the first and possibly most important step towards a more secure system. Attackers should need to work hard to gain even the slightest bit of insight while at the same time doubting if their obtained information is even correct or not. Defenses should be designed on the assumption that there is a breach in the network at all given times. Improving your own ability to collect, evaluate, and transmit digital evidence of attempted attacks or general traffic is a very good short-term cyber defense goal.[15]
Moving away from closed networks and what administrators can do within theirs we have two main deterrence strategies for cyber warfare with three underlying basic requirements which are capability, communication, and credibility [15]:

- Denial: physically prevent an enemy from obtaining a certain technology
- Punishment: last resort strategy in case denial has failed; prevent aggression from an enemy by threatening with greater aggression

Overall, cyber defense is the most important part of cyber warfare. Preparation and foresight are key factors for a more secure system.

5.3 Analyzing the Stuxnet Worm[11][16][17]

To put the learnings of this paper into perspective, we're going to have a look at the Stuxnet worm which is assumed to have been aimed at harming or slowing down the iranian nuclear porgram (uranium enrichment).
Stuxnet is categorized as an Advanced Persistent Threat: It was programmed very carefully and sophisticatedly with the intent of invading a very specific target system, staying undetected for the maximum amount of time, gaining more influence withing the target network while doing harm to it gradually and stealthily. Stuxnet went beyond only stealing information. Instead, it tried to manipulate certain microchips that were responsible for controlling the rotation speed of specific engines of enrichment centrifuges within the plant.
With regards to the in Chapter 2.2 mentioned phases of APT, the following can be said for Stuxnet:

- **Phase 1, Reconnaissance & Weaponization:** There's not much known about how the programmers of Stuxnet got their information, but they most definitely had insider information in various key positions. the level of insight they had to know to get to that level Stuxnet had, is imense. They knew what specific types of engines were built into the machinery as well as what software was used to control those.
- **Phase 2, Delivery:** Stuxnet made use of various zero-day exploits: It impersonated legitimate software by using stolen certificates, it installed itself on the desktop without any notifications via a compromised USB stick once it was plugged into a PC (using a flaw in the Microsoft Windows Operating System to go unnoticed), and, then, seeked out a certain version of the software *Step7* by Siemens and hacked it by applying a secret, built-in password.
- **Phase 3, Initial Intrusion to Phase 5, Lateral Movement:** After a successful installation on one target system, the worm infiltrated the network, spreading out to various other PCs, searching every one of them for the above mentioned specific version of *Step7*. After finding it, it continued on to look for a control equipment called PLC (Programmable Logic Controller) which is responsible for communication between the machinery and the PC. Once it had infiltrated the PLC, it started to check for specific types of microchips. If either of these steps proved to be unsuccessfull Stuxnet stopped its processes on that system and deinstalled itself. A high level of stealth was achieved by the hidden install exploit as well as the use of the seemingly valid, stolen certificate, making the worm appear like a legitimate software. Also, since the program altered the speed in which the centrifuges were spinning and such a modification would have attracted attention, it altered the sensor data, making it look like all processes were running like normal.

Since the goal of Stuxnet wasn't to exfiltrate data, Phase 6 will not be addressed here.
Given the attack strategies of Chapter 5.1 we can classify the Stuxnet worm as a data modification or infrastructure manipulation strategy. Its purpose was to harm machinery (centrifuges) used to enrich uranium. The motivation was most probably political, since it was feared that Iran would use the enriched material to build nuclear weapons.
Overall, Stuxnet had a great impact on the perception of

doi: 10.2313/NET-2017-09-1_10

cyber weapons since it made people painfully aware how vulnerable critical infrastructures can be to cyber attacks.

6. CONCLUSION

Cyber warfare, although seemingly more harmless than regular war, is an increasing threat. The development and growth of interconnected systems, software, and technology in general bears as many risks as it has advantage:

- Cyberwar is cheap: With a computer and Internet access, one can gain knowledge about and access to vulnerable networks.
- Due to the increasing global connectivity, malware is easy to deliver from anywhere in the world.
- Tools for attacking are free and/or open source and openly available.
- The attacker always has the advantage since he can rely on the latest updates and use the newest innovations.
- Anonymity is easily achievable so an attack might be impossible to track back to its source if the adversary is knowledgeable enough.
- Power distribution is extremely disproportional with huge gains for small actions.
- The time between the launch of an attack and its effects is barely measurable.

This list names just a few peculiarities discernible in the concept of Cyber Conflict. In addition, especially regarding open source tools, there is a threat of tools that are not publicly available. With freeware, one can download and analyze the source code, finding weak spots, counter-exploits or ways to defend against them, whereas with private tools, that is not the case.
Future wars will probably involve a mixture of conventional weaponry combined with a number of different cyber weapons. Smaller countries which would have had no chance to compete before can now enter the field, having an impact depending on their know-how and strategic approach. Nobody knows what the future will bring but one thing is for sure: If another war is coming, cyber warfare will be one of the many used with which people will harm and endanger each other.

7. REFERENCES

[1] Igor Bernik, Alan Chong, Stefania Ducci, and Joseph Fitsanakis: *Canada's Cyber Security Strategy. For a stronger and more prosperous Canada* PUBLIC SAFETY CANADA, pp. 3, `https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf`, accessed April 10th, 2017

[2] Jason Andress and Steve Winterfeld: *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2011 Elsevier, Inc, ISBN: 978-1-59749-637-7, USA

[3] John J. Arquilla and David F. Ronfeldt: *Cyberwar and Netwar: New Modes, Old Concepts, of Conflict*, Fall 1995, RAND Review, `https://www.rand.org/pubs/periodicals/rand-review/issues/RRR-fall95-cyber/cyberwar.html`, accessed April 11th, 2017

[4] Andrey Kulpin, Kal Frederick Rauscher and Valery Yaschenko: *Critical Terminology Foundations 2* East-West Institute, Russia-US Bilateral on Cybersecurity, Policy Report 2/2014, - 2014

[5] Ping Chen, Lieven Desmet, and Christophe Huygens: *A study on Advanced Persistent Threats*, iMinds-DistriNet, KU Leuven, 3001 Leuven, Belgium

[6] Ido Kilovaty: *WORLD WIDE WEB OF EXPLOITATIONS âĂŞ THE CASE OF PEACETIME CYBER ESPIONAGE OPERATIONS UNDER INTERNATIONAL LAW: TOWARDS A CONTEXTUAL APPROACH*, The Columbia Science & Technology Law Review, Vol. XVIII, STRL.ORG, Fall 2016

[7] *Gabler Wirtschaftslexikon*, Digitale Fachbibliothek, Springer Gabler, `http://wirtschaftslexikon.gabler.de/Definition/exploit.html-exploit-v3.html`, accessed April 10th, 2017

[8] Robert Axelrod and Rumen Iliev: *Timing of cyber conflict*, Ford School of Public Policy, University of Michigan, Ann Arbor, MI 48109, 2013

[9] Tom Parker, Marcus Sachs, Eric Shaw, and Ed Stroz: *Cyber Adversary Characterization: Auditing the Hacker Mind*, Syngress, 2004, USA

[10] Fyodor and David Fifield: *SecTools.Org: Top 125 Network Security Tools*, `http://sectools.org/tag/sploits/`, accessed April 11th, 2017

[11] Alexander Gamero-Garrido: *Cyber Conflicts in International Relations: Framework and Case Studies*, Engineering Systems Division, Massachusetts Institute of Technology, Explorations in Cyber International Relations, Harvard University

[12] Robin Gandhi et al.: *Dimensions of Cyber-Attacks - Social, Political, Economic, and Cultural*, IEEE Technology and Society Magazine, Spring 2011

[13] Fred Schreier: *On Cyberwarfare*, DCAF Horizon 2015 Working Paper No. 7

[14] Everett C. Dolman: *Pure Strategy: Power and Principle in the Space and Information Age*, London, Frank Cass, 2005, p. 6.

[15] Kenneth Geers: *Strategic Cyber Security*, CCD COE Publication, NATO Cooperative Cyber Defence Centre of Excellence, June 2011

[16] Ran Levi: *Stuxnet: Advanced Persistent Threat*, Curious Minds Science Technology, `http://www.cmpod.net/all-transcripts/stuxnet-the-malware-that-struck-the-iranian-nuclear-program-text/`, accessed May 7th, 2017

[17] Symantec Corporation: *Advanced Persistent Threats: A Symantec Perspective*, White Paper, 2011, `https://www.symantec.com/content/en/us/enterprise/white_advanced_persistent_threats_WP_21215957.en-us.pdf`, accessed May 7th, 2017