Global Scientific JOURNALS

GSJ: Volume 10, Issue 9, September 2022, Online: ISSN 2320-9186

www.globalscientificjournal.com

CYBERWARFARE: A REVIEW OF ATTACK MITIGATIONS AND DEFENSE MECHANISM

EMMAH, Victor Thomas
victor.emmah@ust.edu.ng

UKORMA, Godsfavour
ukormagodsfavour@gmail.com

ORIJI, Ikechi Benibo
ikechi.oriji@ust.edu.ng

Abstract

The world is currently in an era of conflict and cyber-warfare where a nation engages the expertise of hackers to attack vulnerabilities of a rival nation government security systems, financial markets and power grids, and the result of these attacks is as disastrous and devastating as various military arsenals of mass destruction. Cyber-warfare is an Internet-based conflict involving politically motivated attacks on information and information systems which aim to steal or alter classified data, disrupt or disable essential services, disable official websites and networks and cripple financial systems amongst many other possibilities. This paper provides a review of the different methods of attack and defense mechanisms to mitigate and repel cyber-warfare on a nation or organization.

***Keywords**: Cyberwarfare, Cyber Attacks, Cyber Security, Defense, Denial-of-Service*

1. Introduction

Recent advances in technology have completely changed how we live on this planet. Everything can be done in an online world now, from shopping to banking to collaborating on projects. As with all technological advances in history, this cyber world has also been turned into a weapon. It began with individuals pushing the limit of the web or going for personal gain, but now governments have begun to realize that the potential for a cyber-attack is very real, and the resulting damage could be catastrophic. Because of this, several countries are researching and preparing cyber defenses, independently and collaboratively. At the same time, being able to organize such an attack would allow a nation to cripple an enemy without any traditional military action. This has prompted governments to also invest in cyber weapons. Because of the Internet's anonymity, it is easy for an attacker to either cover his tracks or leave a false trail. As such, there have been several large cyber-attacks already that cannot be definitively traced to a country, organization, or person. Only the motives behind the attack and how the attack was performed can give clues towards the aggressor. Before going further, there is need to examine different perspectives and views of cyber-warfare. It should be noted that no definition given about cyberwarfare is most suitable or generally adopted.

Duggan (2001) defined Cyber-warfare as a combination of computer network attack and defense and special technical operations. The definition given by Duggan cannot be faulted rather it can be said to be a broad definition because it does not reveal the entity taking part in cyber-warfare and the reasons for the involvement. Cyber-warfare can also be said to be a conflict between states, but it could also involve non-state actors in various ways (Cornish, 2010). In cyber-warfare it is extremely difficult to direct precise and proportionate force; the target could be

military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target. This definition gives an interesting idea of non-state actors being involved in cyber-warfare. It also emphasizes that cyber-warfare can be imprecise and unpredictable.

Taddeo (2012) defines cyber-warfare as a warfare grounded on certain uses of ICTs within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemies resources, and which is waged within the informational environment, with agents and targets ranging both on the physical and non-physical domains and whose level of violence may vary upon circumstances.

Critically examining the definitions given above, there is a clear indication of the fact that there is no widely adopted definition of cyber warfare. Most researchers present definitions which are very broad and these definitions tend to cover most conceivable cases of cyber warfare but are probably too broad. Others give very distinct definitions that may be more useful but then fail to cover certain aspects of cyber-warfare. The adverse effects posed by cyber attacks can span almost all parts of our lives ranging from negative economic impact, psychological trauma and societal destruction, and even physical or reputational damage.

2. Examples of Cyber-warfare:

There are growing and continuous cases of cyber attacks that has happened all over the world, for example, Killnet, a pro-Russian hacker group, hit several Italian institutions and ministries in 2022. According to Italian cyber-security group Yarix, Killnet launched a series of offensive distributed denial-of-service (DDoS) attacks.

The DDoS offensive targeted websites of the Italian government, judiciary institutions, ministries, and media websites. The Italian embassy in London said the cyberattack disrupted the online process for consular applications (Petkauska, 2022). Other historical reported cases are mentioned below:

- In 1998, the United States hacked into Serbia's air defense system to compromise air traffic control and facilitate the bombing of Serbian targets.
- In 2009, Stuxnet virus was used to attack the Iranian nuclear program. It is among the most sophisticated cyber-attacks in history. The malware spread via infected Universal Serial Bus devices and targeted data acquisition and supervisory control systems. According to most reports, the attack seriously damaged Iran’s ability to manufacture nuclear weapons.
- In 2007, in Estonia, a **botnet** of over a million computers brought down government, business and media websites across the country. The attack was suspected to have originated in Russia, motivated by political tension between the two countries.
- Also in 2007, an unknown foreign party hacked into high tech and military agencies in the United States and downloaded terabytes of information.
- In 2009, a cyber-spy network called "GhostNet" accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world. GhostNet was reported to originate in China, although the country denied responsibility.

3. Methods of Attack

There are many ways to attack a computer or network of computers. In cyber warfare, the method chosen is based on what the attacker's goals are. For example, a nation may want to snoop through a rival's banking system to look for flaws, then they try to take advantage of the flaws so as to cause economic instability. The ubiquity of computers basically guarantees that whatever an aggressor want to do to a target, he can do, as long as he uses the right attack and has an intelligent group of people to organize it. In order to attack the opposition's system, the attacker gains access to the system, then installs malicious software which might be used to spy on them and then strikes. Some of the methods of attacks in cyber warfare are described below.

I. Gain Access

The attacker gains access to the system by

- ✓ Exploiting the security gaps in the software programs installed on the system
- ✓ Hacking of passwords which is increasingly done automatically (brute force)
- ✓ Intentionally misleading of users by social engineering e.g Wrong administrators asking users for passwords.
- ✓ Using manipulated emails with malicious attachments and links to websites containing malware. This is known as phishing. Phishing is a method where users are misled to a malicious website by masquerading as a trustworthy entity to acquire sensitive information.
- ✓ Infected data storage media (such as floppy and hard discs, DVDs etc).

II. Malicious software (Malware)

All computer users know that malware is bad. However, many users aren't good at avoiding malware. Because governments employ many people, chances are good that at some point, some government computer will get infected. What happens after that, depends on what it was infected with. For example, in mid-2009 a virus now known as Stuxnet began to infect computers around the globe. Symantec, an antivirus corporation, noticed and catalogued it, but it didn't get much attention because it wasn't causing any problems. A small security company in Germany began investigating it and found out that the virus would only cause problems in very specific circumstances. Ralph Langner, the owner of the security firm, said "It was a marksman's job". A few months later, the virus struck. Nearly 1000 machines responsible for enriching uranium in Iran were destroyed.

Enriched uranium can be used to create nuclear weapons, and the destruction of the equipment caused a major setback in Iran's nuclear program. Stuxnet appears to have been targeted at that equipment. When it was on the computers responsible for those machines, it first waited and gathered data from the normal operations. Then, it caused the machines to lose control and destroy themselves while reporting that everything was fine. Stuxnet has been called the "most advanced cyber weapon ever deployed".

In late 2011, a new virus, DuQu, was found by Symantec. At first it was classified as Stuxnet, but they realized it was something else. Stuxnet just used other computers as a way to get to its target. DuQu, however, was gathering information on every computer it infected. It stayed on each computer 36 days profiling the computer and the network and keeping a log on all keystrokes. It sent all this information off to a secure server, and when its time was up it removed itself. Because it was just discovered, no one knows how many computers it has gathered

information on or what the information will be used for. However, it is likely that it was gathering information in preparation for some sort of attack.

III. Denial of Service

A denial of service attack, is a method of attack that aims to disable a server or network by flooding it with messages. If the attack is successful, the target will be unable to deal with all of the incoming traffic. The target will then most likely crash or reboot. Depending on how the system is set up, this may in turn cause damage to the server or applications running on it. The main goal of a denial of service attack, however, is in its name; it denies legitimate users access to the system. This makes it a fantastic propaganda tool. Average users wouldn't have any idea what's actually going on; all they know is that the site or service they wish to use won't respond. They realize there's something wrong with the system, and they lose confidence in it. Such an attack can cost a company millions in lost revenue during the outage, plus the cost to repair damage and the loss of users in the long term. When used in warfare, the effects of a denial of service attack can be even more dangerous. Because people are so used to having access to lots of information at all times, an attack on a government or news site can cause panic. The effect is multiplied if the attack is done during a time of turmoil, such as during an aggressive military action or civil unrest. Furthermore, the citizens of the afflicted country may turn to other sources for information, giving the aggressor an opportunity to spread its propaganda. If government or military communications centers are attacked, the target country's leadership will be unable to coordinate to figure out what is happening. This lack of response will cause even more fear amongst the population and within the government.

In a traditional denial of service attack, an attacker uses a single machine to repeatedly send messages to a target, using up its bandwidth and completing the attack. However, this is no longer practical for several reasons. First, most large servers and any worthy cyber warfare target would have a large enough bandwidth to handle a single machine, unless it was another large server. This is generally not the case, so in most cases the target would actually be able to handle the attack, even if its service is somewhat slowed for the duration. Secondly, most servers only allow a certain number of requests in a given time period from a single machine. This means the attacker would soon start to have his messages rejected, defeating the attack.

Finally, the attackers IP address would be well-documented after the attack and easy to track down. Single machine Denial of Service attacks are no longer used because of these weaknesses. Today, the most popular form of Denial of Service is a distributed denial of service attack, or Distributed Denial of Service. The figure below shows an example of a Distributed Denial of Service attack.

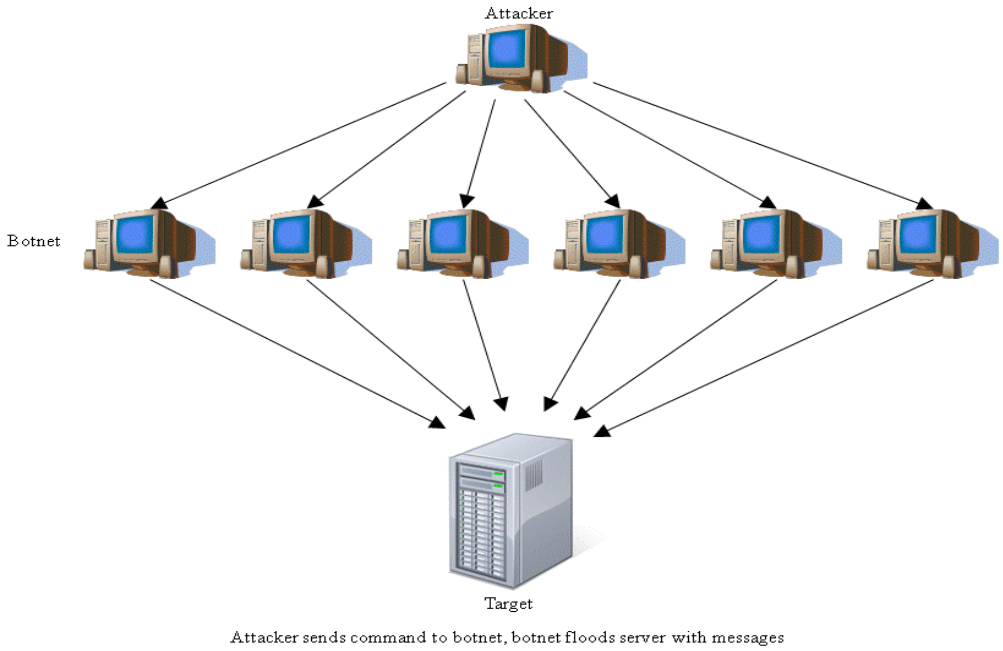

Figure 1: An example of a Distributed Denial of Service Attack

The principle is the same as a traditional Denial of Service attack. However, instead of a single computer, hundreds or thousands of computers are used. These are often privately owned computers infected with a virus, so tracing them to the attacker is impossible. Because they are so many, the target cannot block them all before crashing. Some people involved cybercrime make their living by controlling large botnets, which are collections of infected computers ready to flood a target whenever the command comes in. Botnets can often be rented for pennies per computer, making them a cheap and effective way to disrupt a nation's communication and cause unrest in the population.

The only problem a government would run into while using a DDoS attack is how to get a botnet. If a government tries to create its own botnet and is discovered, it would result in serious crises. If it rents from a cyber-criminal, the attack may be traced back to the country that ordered it if the cybercriminal doesn't stay quiet. However, governments with the means and motive to hire a botnet will probably be able to cover their tracks. As such, there have already been DDoS attacks allegedly linked to different countries of the world, but none has been proven to be true.

Another form of DoS attack is a permanent denial of service attack, or PDoS. This attack is specifically designed to damage the target's hardware, rather than just crash or deny access. It does this by corrupting the target's firmware. After this, the hardware must either be flashed with new firmware or replaced. Either way, the targeted system is taken down for a long period of time after a quick connection. This attack would only work on devices that can be flashed over a network: most likely an unsecure router or switch.

In general, to be successful in carrying out an attack, an attacker follows these step illustrated below

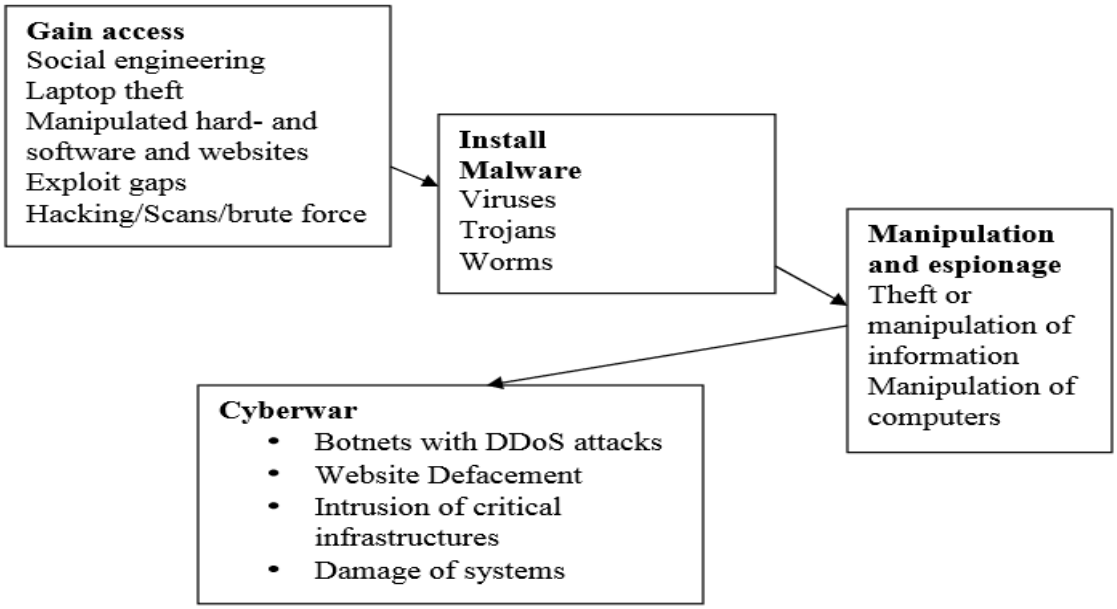

Figure 2: Cyberattack Execution Process

4. Methods of Defense

Defending a network from attackers may be classified into active and passive defense. These are explained in the following sections.

I. Active Defenses

Active defenses take action to prevent or retaliate when the system is attacked. The Pentagon describes it as introducing military concepts such as organizing, training, and equipping its personnel and using strategy to defend its cyber resources. One form of active defense is called a honeypot. With a honeypot a fake network is created and attached to the network that is being protected. Some security holes are left open, but it's kept secure enough to make the attacker think it's a network that's in use. The administrators can then track the attacker and his actions. From this, they can often tell what the attacker is after and how skilled the attacker is. If the attacker is particularly careless, it may be possible to trace him and find him. This opens up the possibility of retaliating against the attacker.

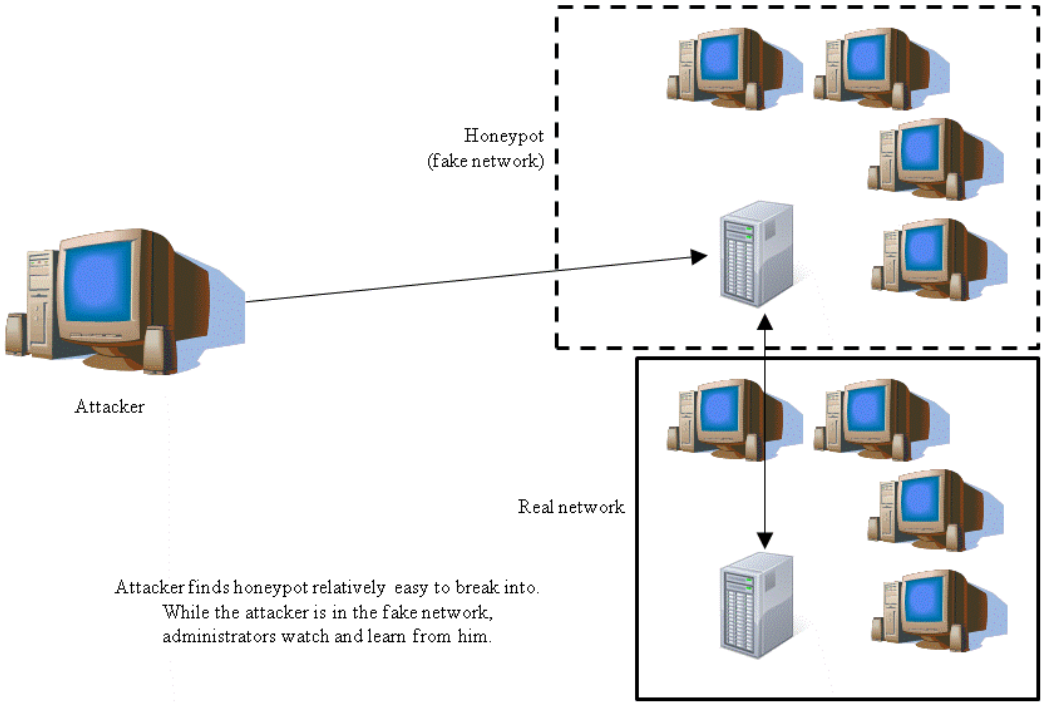

Figure 3. Active Defense Mechanism

Because DDoS attacks are so easy to perform and can cause huge problems, there has been a lot of research into preventing a DDoS attack from taking down the target. This is a difficult task, as the goal of DDoS is to overload the system. If the attack gets that far, the target may not be able to call for help or have the resources to deal with the attack. So, prevention is the best way to deal with it. DDoS can be prevented by carefully filtering packets before sending them to the server. If a router can recognize that it's getting similar messages from the same location, it should not transmit them to the server. Also, a firewall can be installed that only allows network traffic on approved ports. This is still vulnerable, but not as vulnerable as system with all ports open.

In some systems, a DDoS attack can be detected and mitigated so that the server withstands the attack and stays online. There are two general ways to detect a DDoS attack. The first is based on previous knowledge of what DDoS attack looks like. If the same signature occurs, it means the system is probably under attack. The second creates a profile of normal activity. If activity deviates from that profile, the system may be under attack. Using the second method, anomaly based detection can detect previously unseen attacks, but it can also result in generation of more false alarms.

So how do you protect your company's servers from the onslaught of data sent from infected PCs across the Internet? How do you keep a DDoS attack from bringing down your company's network? There are several approaches you can take to defend against a distributed denial of service (DDoS) attack:

Black-holing: This approach blocks all traffic and diverts it to a black hole, where it is discarded. The downside is that all traffic is discarded -- both good and bad -- and the targeted business is taken off-line. Similarly, packet-filtering and rate-limiting measures simply shut everything down, denying access to legitimate users.

Routers: Routers can be configured to stop simple ping attacks by filtering nonessential protocols and can also stop invalid IP addresses. However, routers are typically ineffective against a more sophisticated spoofed attack and application-level attacks using valid IP addresses. Firewalls can shut down a specific flow associated with an attack, but like routers, they can't perform anti-spoofing.

Intrusion-detection systems: Intrusion detection system solutions will provide some anomaly-detection capabilities so they will recognize when valid protocols are being used as an attack vehicle. They can be used in conjunction with firewalls to automatically block traffic. On the downside, they're not automated, so they need manual tuning by security experts, and they often generate false positives.

Distributed Denial of Service mitigation appliances: Several companies either make devices dedicated to sanitizing traffic or they build distributed denial of service (DDoS) mitigation functionality into devices used primarily for other functions such as load balancing or firewalling. These devices have varying levels of effectiveness. None is perfect. Some legitimate traffic will be dropped, and some illegitimate traffic will get to the server. The server infrastructure will have to be robust enough to handle this traffic and continue to serve legitimate clients.

Servers: Proper configuration of server applications is crucial in minimizing the effect of a distributed denial of service (DDoS) attack. An administrator can explicitly define what resources an application can use and how it will respond to requests from clients. Combined with a distributed denial of service (DDoS) mitigation appliance, optimized servers stand a chance of continued operations through a distributed denial of service (DDoS) attack.

Over-provisioning: Buying excess bandwidth or redundant network devices to handle spikes in demand, can be an effective approach to handling distributed denial of service (DDoS) attacks. One advantage of using an outsourced service provider is that you can buy services on demand, such as burstable circuits that give you more bandwidth when you need it, rather than making an expensive capital investment in redundant network interfaces and devices.

II. Passive Defenses

Passive defenses don't search for problems on the computer. Instead, they try to prevent the computer from being attacked in the first place. Examples include firewalls, antivirus software, and access control. Firewalls monitor incoming connections and deny those it deems dangerous or untrustworthy. Antivirus software can scan the files that are allowed through to be sure they aren't hiding malicious code. Finally, access control assigns users and computers to different permission categories. This can prevent a compromised computer or user account from damaging the entire network. Most companies have each of these (firewalls, antivirus software and access control) implemented on their network or computers.

There are various problems with this approach to security. First, each of these security measures reduces usability as it increases security. The most secure system would allow for no input, but it

would be totally useless, while an entirely open system would be user-friendly but infected in minutes. Secondly, an attacker only needs to find one point of entry to compromise the system. From the entry point discovered, he can often turn off the other defences (with the exception of access control). Points of entry can come from user's error or flaws in the security programs. This requires an unending series of patches and updates along with repairs, which cost a lot of time and money.

5. Conclusion

The techniques and technologies discussed in this paper are just a tip of the iceberg of the methods that can be used to steal information for fun or profit. As competition in the global market place increases, so will the instances of corporate espionage. Therefore, companies both big and small need to take necessary steps to protect themselves from becoming a victim. Here are four necessary steps to help protect valuable data from falling into the hands of competitors.

1. Companies must identify what information is sensitive and classify it as such. Information such as R&D processes and innovations or new market strategies are easily identified as "sensitive." However, other information such as personnel files, pricing structure, and customer lists are often overlooked and left unprotected.
2. A company should regularly conduct a risk assessment to identify vulnerabilities, and to tackle these vulnerabilities so as to avoid the probability of someone exploiting them and obtaining sensitive information.
3. Establish, review and update security policies and appropriate safeguards, both procedurally and technologically, to thwart attempts to exploit vulnerabilities and gain access to valuable company data.
4. Train all employees. Users, managers and IT staff all need to be trained so as to enlighten them on the business information that needs to be safeguarded, techniques that can be used to gain access to sensitive data, and procedures that should be taken to report suspected attempts by illegitimate users to gain access to sensitive information.

"People using computers and the professionals maintaining networks and systems are the source of the problem, which means that training all employees is an essential step in managing an IT security program. Users who are not trained to detect phishing and pharming attacks can open dangerous backdoors to hackers." Knowledge is key. The more knowledge a corporations have about the threats that are out there, the better they will be able to defend themselves from attempts to steal sensitive information.

The most effective protection against cyberwarfare attacks is securing information and networks. Security updates should be applied to all systems including those that are not considered critical because any vulnerable system can be co-opted and used to carry out attacks. Measures to mitigate the potential damage of an attack involves comprehensive disaster recovery planning that includes provisions for extended outages.

References

1. Petkauska, V. (2022). Hacker wars heat up as the pro-Russian Killnet attacks Italy. Retrived from *https://cybernews.com/cyber-war/hacker-wars-heat-up-as-the-pro-russian-killnet-attacks-italy/*
2. John, M. (2011). Israeli Test on Worm Called Crucial in Iran Nuclear Delay. *The New York Times*.
3. Chad Nelson (2011); Cyber warfare: The newest battlefield

4. Dave, D. (2003); Economic Espionage and Trade Secret theft: Defending against the pickpockets of the new millennium. *The 2002 Annual report to congress on foreign Economic espionage and industrial espionage*
5. Froutan, P. (2004); How to defend against DDOS attacks; *an article published by www.computerworld.com*
6. McDowell, M. (2009); "Understanding Denial-of-Service Attacks," US-CERT. .
7. Shane W. R (2003); Corporate espionage 101. SANs Institute publication, version 1.3
8. Shane W. R (2007); Corporate espionage 201. SANs Institute publication, Version 1.0
9. Saalbach, K. (2015); Cyberwar: Methods and practice. University of Osnabruck Publication
10. Clarke, Richard A. (2010); *Cyber War*, HarperCollins (2010) ISBN 9780061962233
11. http://searchsecurity.techtarget.com/definition/cyberwarfare
12. https://en.wikipedia.org/wiki/Cyberwarfare
13. https://en.wikipedia.org/wiki/Industrial_espionage
14. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html
15. http://www.us-cert.gov/cas/tips/ST04-015.html