Cyberwar - Just “Warcraft in Space”?

Nico Maas
Seminar “Angewandte Informatik”
Hochschule für Technik und Wirtschaft des Saarlandes

***Abstract*—Cyberwar is a buzz word used widely in media today, but a definition for the phenomena has never been established. What is Cyberwar? What does Cyberwar include or imply? Is it like real war and if so, where does it take place? Which corporations do deliver the needed weapons and how do they look like?**

I. Introduction

“One problem is that there’s no clear definition of “cyberwar.” What does it look like? How does it start? When is it over? Even cybersecurity experts don’t know the answers to these questions, and it’s dangerous to broadly apply the term “war” unless we know a war is going on.” [1], says Bruce Schneier, an expert on Cybersecurity. The problem we see here is, that even an expert in this field cannot answer these questions, but even gives more aspects into consideration. Because the concept of ”Cyberwar” is so complex a logical approach would be to apply the scientific method. When examining the concept of ”Cyberwar”, it appears to be a neologism of the words “cyber” and “war”. According to the Cambridge Dictionary cyber is defined as: “involving, using or relating to computers, especially the internet” [2] while war is explained as “armed fighting between two or more countries or groups” [3]. By combining these two meanings, we understand the term to mean a war which is conducted via computers and the Internet. Keeping Schneiers statement in mind it seems likely cyberwar is similar to war itself.

II. Traditional War

Traditional war has several properties and methodologies which are applied. A war is normally fought between different countries in order to achieve a goal such as: weakening the influence of the enemy party, gaining territory, or destroying valuable assets. To achieve these goals several methods are applied. Sabotage could be used to prevent the success of a competitor, while espionage helps with identifying enemy tactics and data. In addition to the parties and chosen war tactics there are three common keystones in war - first, a war is declared, then it is reduced to a specific location, and there are armaments. The declaration explains to the opposing country and it could also explain the reasons which led to the war. Secondly, a war is in most cases reduced to a specified battlefield, where the fighting takes place and is decided. Lastly, there are special stakeholders, called armaments which are responsible for delivering specialized tools (usually specific weapon types) to fight the war.

A. Earth

While traditional wars are fought between countries they are not usually expanded beyond its borders. The face of war is changing rapidly. Now there are several groups which declare war against countries, ethical groups, or persons. These so-called terrorist groups could not lead a traditional war as they are not a country by definition and as such they do not work within defined areas or borders, nor are they different from military or civilian. In truth it has become very difficult to differentiate a combatant from a civilian because terror group combatants are not marked as such as they are not visible in military dress. Because of their ability to blend in they are able to attack targets without warning. Even some traditional wars, for example - Vietnam, were never started directly by the attacking countries. With these facts in mind cyberwar will be examined by comparison.

B. Internet

In regard to the Internet in terms of cyberwar there a several important points which come to mind. The most important is that the Internet is not owned by a specific country or corporation. It is de-centralized and has no borders or limitations by nature as a world-wide network. In addition this also means that there are no borders in terms of attacking other persons, companies, or even countries. There are distance limits with conventional weapons. But cyber-weapons can reach their target instantly no matter their location. There aren’t needs for specialized technologies such as multi-stage intercontinental missiles; it is simply finding a vulnerability in common used software that is sufficient to take a website offline or the database system of a competitor. Another advantage of cyber-warfare is it is also not necessary to hire several specialists, gain access to restricted areas, or obtaining rare materials like uranium. A war like this can be fought with just one person on a normal laptop with internet connection. Therefore, a cyber-threat could originate from anywhere. Because the internet is de-centralized it allows the attacker to stay unknown and to disappear after completing their attack.

III. Methodologies

The following section should point out several methodologies used in traditional Warfare and apply them to cyber-warfare.

A. Sabotage: Stuxnet (2010)

One of the most noticeable acts of sabotage was the Stuxnet attack in 2010. Stuxnet was a computer Trojan virus that was

developed to attack the Uranium Enrichment Centrifuges in Natanz. By targeting the Siemens Simatic Step 7 software and a special configuration of Step 7 CPUs, Controllers and Motors, the software was able to pinpoint its target and only attack the desired structure. This software was deployed by USB stick and could self replicate over different networks by using Zero-Day vulnerabilities in several different Types of Microsoft Windows Operating Systems.

By Zero-Day Vulnerability, a bug in a software is meant, which is unknown and therefore unadressed by the developer team. There are several cracker groups which are looking for exploits and software bugs. These are usual held in secret to create new malware, or sold to other groups and companies. Because of the fact that most of these found bugs are used the same day to create an attack or malware - they are called "Zero-Day", as no day has passed since the problem was found. Because the exploited problem is unknown to the software developers or other security experts, the chance that these holes could be used successfully on an "first strike" is quite high.

After infecting the target computers of the correct Step 7 configuration, Stuxnet applied itself on the Step 7 CPUs and started to alter the spinning speeds of the uranium enrichment centrifuges.

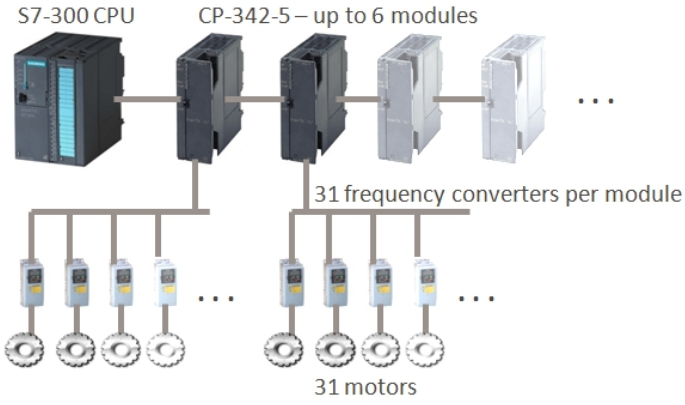

Figure 1. Stuxnet Target Configuration [4]

By tampering with these controls in terms of decreasing and increasing the speeds from 2 Hz to over 1400 Hz, the Trojan damaged the centrifuges over several months and they eventually failed. Because it was only attacking certain centrifuges it could disguise its work and stayed undetected over a period of nearly a year. By the time it was detected it had already destroyed several hundred centrifuges and reverted Iran's atomic program by years. The Trojan itself (Stuxnet) is a highly sophisticated piece of software. Security software company Symantec pointed out that it could not be a piece developed by some programmer because it was too complex. They suggested that it had been created by one or more countries. It is rumored that the software had been developed by the United States in cooperation with the Mossad (Israel intelligence agency) specifically to target the Uranium Enrichment Centrifuges in Iran and hindered their atomic program from succeeding.

B. Sabotage: Conclusion

This attack clearly shows the possibilities of cyber-weaponry like the Stuxnet Trojan. It is very flexible and can reach its target over multiple attack vectors: i.e. a USB Stick, internet download, or another network infrastructure. It is a sophisticated attack because it only attacks its target and uses non-targets to deploy itself to other computers in order to find its designated system. It has the possibility of hiding its presence by erasing itself after a period of time or successful deployment on a non-target system. It is a more effective weapon than using a missile or bomb because they are more precise, it will reach its goal without revealing its creator, and is far more elegant in terms of evading collateral damage. The ability to be anonymous could prove very valuable for corporations or states. They could potentially attack, manipulate, or destroy a target without proof of origin; which in turn could lead to a new way of "cold war" warfare.

Putting the efficient use as "smart weapon" aside, in cases of sabotage, attacks with cyber-weapons can be just as devastating as any other conventional weapon system. The occurrence of such attacks will increase with the incline of computerization and integration of networked systems into our daily life. Given the fact that the United States of America as well as multiple European nations are working on a so called "smart grid" to control and improve their electrical grid - it gives new opportunities to hackers. An example would be the new "smart meters" which are expected to be installed into every home in order to measure and conserve the amount of used electrical energy. With this data, a profile of a person could be created, which is problematic - as it can show wheter the person is living at home, or on vacation. In the later case, burglars could use the chance to break into the household and steal goods. Even more problematic, these "smart meters" can also be supplied with control functions [5], i.e. such as shutting off selected electrical outlets, or even taking complete households offline. This is very convinent in the case of remote controlling home appliances via Smartphone, but it can also have severe consequences if this functionality is exploited by an hacker or terrorist group. Additionally, the computerized and networked smart meters are also vulnerable to similar problems as normal operating systems: So called "smart meter worms" do already exist in labs and have already proven in simulated attacks to be very effective. [6]

C. Espionage: F-35 Lightning II (2009/2011)

In terms of Cyberwar espionage the case of the F-35 Lightning II or "Joint Strike Fighter" comes to mind. The USA started to develop a new tactical aircraft to replace the F-16 which had been in service since 1974. The United Kingdom, Italy, and Japan are also participating on this development, among others. In 2009 the first case of espionage regarding this project became known. Hackers stole several terabytes of data regarding this aircraft. [7] In 2011 a similar incident took place: The two factor authentication mechanism of RSA was

breached, rendering the specialized Token generators, relied upon by many corporations within the security and banking sector, useless.

Figure 2. RSA SecurID Keyfob [8]

Among those corporations was also the main developer of the JSF System: Lockheed Martin. [9] Another security breach with large scale data compromitation was detected just shortly after the successful attack on RSA. A two factor authentication means that the authentication does not rely solely on a username and password, but also on a dynamic factor. In this particular case it relied on a dynamically generated number selection - created by a key fob from RSA. This generated number is only valid for a limited amount of time, in most cases about 1 minute. After that a new key is generated. Breaching the RSAs second factor makes attacking a secured system a lot easier. Using two factor authentication could potentially give the impression of a full security to a user while reducing the importance of strong and secure passwords. In case of such an attack, that renders the dynamic factor useless, a very weak password could give access to an otherwise highly secured and sensitive network. This was most likely the cause even though the enforcement of strong password rules in security related corporations normally should prevent this.

D. Espionage: Conclusion

The result of these cyber-attacks and these types of espionage were devastating. It was recently revealed that the project has been delayed several times in the last few years because of multiple attacks and data theft. The hackers gained access and insights about the system which could reduce the effectiveness of counter measurements or computer systems of the plane. Therefore a redesign of critical elements or patches to software problems are necessary. Because of this extensive security measurement the price for a single plane jumped from 156 to 207 million US Dollars, as well as delaying the program, and the delivery of the planes to the troops. There is no way of telling whether the stolen data had been sold to terrorists; or those who want to develop counter weapons or exploit flaws in the highly computerized weapons system. This case of espionage and data theft may be not the simplest, but considering the overall damage and past successes, it could potentially be one of the most dangerous. We must consider that the long-term consequences of these events are yet to be seen. The interesting fact about this case is that it is an attack that can be completely seen as a case of cyber-crime, made only possible by the existence of the internet / networked computer systems.

E. Weapons: Reaper (2009/2011)

The Weapon Reaper is an interesting example of a cyber-weapon because, not only relating to computer viruses or attacks, but also how future weapon systems will be designed, controlled and used by networked computer systems. The Reaper is the armed version of the US Drone Predator which has been used in several wars for spying on enemy troop locations and movements. The Reaper has been developed to not only have a longer operating time but also to carry Air-to-Ground Missiles and Weapons. These drones are not only able to watch the battlefield from above but also actively attack a target on sight. It is said that these drones flew more than 230 missions, taking the lives of more than 2000 human targets. But these Drones also proved to be vulnerable to multiple cyber-attacks.

During 2009, multiple Laptops with video footage from Predator and Reaper drones were found in the hands of terrorist cells. After inspecting and tracing back the material it came to be known that the terrorists were hacking into the spy planes. They were able to warn other terrorist cells and groups to evade potential attacks because of a design flaw in the drones: The first downlink of the drone is unencrypted. Predator as well as Reaper drones relay their video and control signals via antenna to a ground station before these re-transmit to the control stations in the US via satellite. Because of the unencrypted signal of the video system and standard protocol terrorists could receive and use the video signal with off-the-shelf video software for 26 US Dollars. [10]

Another security problem arose in 2011. The US Air force became aware that their ground control stations had been infected by a key logger. [11] The program itself could be removed, but it had been installed for more than two weeks. It did not damage or influence the missions, but it could also not determined where the infection arrived from. It was determined that this malware was a software designed to steal the login credentials of users of the game "'Mafia Wars"'. How this malware ended up on the ground control systems remained unknown. [12]

The last known problem with drones occurred in the end of 2011. Iran claimed to have "'taken hostage"' an RQ-170 Sentinel, one of the latest and modern drones of the USA. They pointed out it occurred by the jamming the control signal from the ground control station which forced the Drone into autopilot mode. While normally it would simply return to home base, Iran had disrupted the GPS signal and landed the Drone in their territory. [13]

As this sounds very easy, it is important to further understand the function of the GPS System to evaluate this accomplishment. After being forced into autonomous mode, the Drone would try to return to its home base via the use of the Global Positioning System, GPS. This system uses more than

24 specialized satellites, stationed in earth orbit and equipped with an atomic clock and an transmitter. By combining the received data from these satellites, the difference in signal recievement times and the knowledge about the fixed positions of these satellites, the GPS Receiver can pin point the position of the object on the globe.

The position data is sent over multiple frequency bands: An higher accurate and encrypted military signal, as well as an less accurate and unencrypted civilian frequency. As the encrypted military signal band could not be tempered with, it is very likely that this special band had been jammed as well, which is possible as the signals from space are very weak and could be “overwritten” by an high power antenna. Cutting of the military, encrypted GPS Signal must have forced the GPS Receiver into fall-back mode, as well â which would relay on the unencrypted, civilian signal - if usable. And this signal could be altered and simulated by specialists. In the end, it would be possible to hijack the drone, as already shown by a group of researchers from the University of Texas, but it would be very hard to achieve. [14]

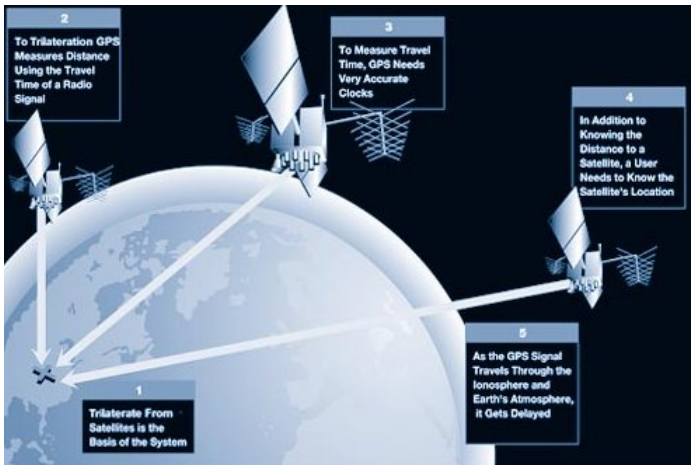

Figure 3. How GPS works [15]

Whether the Iran was able to recover the Drone by this kind of cyber-attack or because of a defect cannot be said for sure, but it is true that the drone has been reported lost by the USA. Iran did also back their story by providing images of the drone as well as data, alleged from it, naming different service dates and inspections noted in the memory system of the Sentinel.

F. Weapons: Conclusion

Considering the use of drones as future weapons or cyber-weapon systems give concern to multiple issues. Drones, it is often argued, provide protection for soldiers on the battlefield. There is no need to put an air force pilot in danger, if you can achieve the same results with an unmanned air vehicle, or UAV. In fact, drones have a longer range and can achieve longer mission durations. However, the problem from an ethical point of view is, that these kinds of missions resemble a videogame; especially watching the cameras in green-night-vision mode. Drones also link traditional warfare and cyberwarfare in a way possible no other system does - by engaging in war on the battlefield by using Software Tools. But drones are also sensitive to cyber-attacks as shown here. There is no assurance that a drone could not possibly hacked in the future and be used against its own civilian targets. At the same time, it makes also one point certain: cyber-weapons such as Stuxnet cannot be controlled or regulated by means of laws or sanctions. There is no possibility to trace a cyber-weapon from space, as done with nuclear warheads and material. [16] They also can be developed with very few experts and do not need specialized tools which could be regulated. Because of which they could potentially overcome traditional weapons in terms of potential damage, especially when considering the effects it could have on the industrial infrastructure.

IV. Stakeholders

One of the biggest groups of stakeholders in warfare, besides the involved countries and people, are armaments corporations. One of the driving factors of technological development is warfare itself. If we consider cyber-weapons or cyber-warfare and want to provide their use and existence then there must be specialized technological corporations which provide armaments. A list of such companies has already been created and is regularly updated by the Stockholm International Peace Research Institute, SIPRI. The SIPRI TOP 100 [17] lists the TOP 100 arms-producing and military services companies. This list clearly shows the existence of multiple computer corporations on this, including their ranking. Hewlett-Packard i.e. rose from their rank 51 in 2009 to place 32 in just one year, as well as NEC which made it from place 77 to 70, while traditional armaments corporations like ThyssenKrupp or Kraus-Maffei lost places. It would have been even more interesting to see the development in the following years, especially in 2011 and 2012 to find out whether the involvement of such corporations had grown after the Stuxnet incident. One indication from this data is certain â that the growing importance of computer corporations. One special case, the story of Samsung Techwin should be mentioned here.

A. Samsung Techwin

As a result of history, many corporations in industries such as car manufacturing or the maritime sector has been involved in several military projects. It is no secret that well-known brands like Rolls Royce or Daimler Benz have been and still are very active on the military market by producing engines and other products for tanks, planes, and other military grade usage. The reason why this happened is easy to explain: These corporations were the only ones with the knowledge and ability to produce the needed goods in times of war. Today, there is no active world war, but there is a need for specialized equipment in terms of cyber-warfare or computers / networked systems - and a lot of money attached to that need. As a result corporations like NEC or Samsung created their own military research departments which only develop solutions for the military market. In the case of Samsung, or Samsung Techwin the consequences were severe. In 2006, Samsung

Techwin built their first turret called “SGR-1”, unnoticed by the western government and media. This turret system allows its users to survey a border to a distance of 4 kilometres via CCD Cameras and infra-red, it is armed with an 5.56 mm gun (developed and build by the car manufacturer Daewoo), which allows this system to effectively secure such protected points. [18] All turrets are controlled over a central ground station and their weapons can engage automatically after authorization via the “kill-switch” by key. These turrets were not developed for lab conditions, they have been installed in the same year at the Korean border and are now “protecting” several kilometres. [19] Samsung has been very quiet about this development because they likely fear alarming their citizens, in addition to potential customers of their mobile and tablet sectors.

B. Stakeholders: Conclusion

As already shown there is not only the need for specialized cyber-weapons but there also enough contractors from the consumer market willing to provide them. It is not only the case that former plane manufactures started to assemble drones (as in the case of the Predator and Reaper Drones), but also computer companies which joined the military sector in the hunt for profitable new markets. So, in terms of specialized equipment, we could prove our questions for these special armaments corporations in the meaning of cyber-warfare and cyber-weapons. The question is, whether the consumers will like a corporation which does not only develop sharp smart-phones, but also uses these resources to produce piercing weapons systems. But this is in their mind to decide.

V. Politics

As a normal war defines itself about separate countries, leading and declaring war against each other, it is necessary for the recognition of the government and politics to accept cyberwar as a real case of warfare.

A. Article 5 of the Washington Treaty

“The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.[...]” [20]

The Article 5 of the Washington Treaty does describe “the principle of collective defense”: It means that, if one of the NATO partners is attacked by an armed force, the NATO partners are to support the victim in restoring peace, by all means necessary - including the support with weapons or troops. This kind of action has already taken place in the case of the terrorist attack on the World Trade Center, United States of America as of 11.09.2011. However, even given the fact that countless cyber-attacks have already taken place, until now, the Article 5 has not yet been used to defend the country via the means of an armed attack. Naomi Joseph of the Canadian International Council believes that this is because of two facts: First, it is very hard to determine the origin of a cyber-attack. By nature of the IP or Internet protocol, it is quite easy to reroute traffic and disguise an attack, sending it over another country or location. So there is quite a bit of uncertainty whether a traced down IP Address is really the source of the attack, or just another disguise or culprit. With no prove or certainty about this fact, the use of Article 5 is already unrealistic. And Joseph’s second point makes the situation even worse: Article 5 was designed to help nations in an armed attack, i.e. an attack where human lives were endangered. An real prove, whether an cyber-attack on US or Allied Ground did already cost human lives, is still missing and unclear. [21] Because of these two facts, Article 5 has not yet been applied to an cyber-attack, rendering the meaning of the word “cyberwar” more to an conflict than real war scenario. However, even though cyberwar has not yet been recognized in the NATO as an equivalent to a traditional war, it does not mean that separate countries would not take these risks seriously.

B. Cyberwarfare Defense Center

In the last years, multiple governments around the globe started to create so called “Cyberwarfare Defense Centers”. These specialized groups exist solely for the purpose of guarding the country and the own armed forces from the cyber-attacks of other countries or common cyber-threats like new worms, Trojans or similar malware and scam. This also includes the evaluation of counter measurements to defend the systems in case of an attack or even strategies to attack an foreign country by the means of cyber-warfare.

Reason for this development lies in different factors. Most countries like America did suffer from recent and growing attacks and espionage, as already shown in the last sections. But it is not only America: Another good example would be Japan, which biggest military contractors Mitsubishi Heavy Industries and Kawasaki Heavy Industries security had been breached several times, losing important documents in the process. [22] Fact is, that little countries could potentially start to pose a big security threat, which could not be seen ahead, as cyber-weapons cannot be controlled and regulated like normal arsenal.

But Japan would not be the last country to go to such measures: Alarmed by the recent events in terms of the F-35 Lightning II and the Stuxnet Worm, Germany founded their own Cyber Defense Center in 2011. This Institution is directly linked to the Federal Office for Information Security (BSI), as well as the German Army / Bundeswehr. [23]

Last but not least could the same development seen in the United States of America, where the so called “Cyber Command” was founded in 2009 - and clearly shows the point the be proven here: Cyber Security is a real threat, taken seriously by the governments of the world. The here mentioned US Cyber Command should increase its personal

capacity from 900 to 4500 persons, as noted by the Spiegel [24] in January 2013.

But this kind of control is not enough: In some cases politicians called for an "'emergency switch"' for the Internet, meaning the possibility to shut down the country from the Internet in a special emergency case. These demands were also made by United States President Obama - and declined multiple times. [25]

In other countries were censorship by government is common, these buttons already exist. In the case of the Arabian Summer i.e. Egypt did cut the connection to the Internet, trying to prevent the citizens from exchanging information by the short messaging service Twitter. [26]

All these cases show that cyber-crime and cyber-security is taken very seriously by the governments. At the same time, however, we can clearly see that it is tried to use this fear to install new means of censorship and control - sometimes as it seems - even by the means of making risks appearing greater than they actually are.

VI. Conclusion

The goal of my work was to explain the concepts, used methodologies and tools in cyberwar and to examine whether cyberwar could be seen as war, or something different.

Our first comparison led to the methodologies of war: Stuxnet, as an example of sabotage through cyber-weapons, has proven to be an excellent demonstration of the possibilities these tools offer: The attacker could stay undetected, influence the development of the nuclear program on a massive scale and even avoid human loses on both sides as well as further complications or counter-attacks.

In the case of espionage, the case of F-35 Lightning II had proven that even armaments and security corporations of the United States of America are not secure from attacks by cyber-weapons and eavesdropping. The loss of the delicate data of one of the most advanced weapons systems as well as the future consequences of this incident are yet to be seen.

As cyber-weapon and target of cyber-attacks, the Reaper and Sentinel Drones haven proven to be a double-edged sword. On the one hand, they protect the lifes of own military personnel and play an important part in reconnaissance missions. I.e. the here mentioned Sentinel or RQ-170 was the drone used to spy on the Bin Laden hideout, which got it the nickname "The Beast of Kandahar". [27] On the other hand, if the information captured by these drones can be that easily accessed by enemy troops, it could be of great disadvantage and even put the life of the own soldiers at risk. At the same time these drones haven proven to be an excellent weapons system, as well as an dire warning to the risks an computerized weapons system faces.

Thinking about stakeholders, the SIPRI TOP 100 clearly shows that there are multiple armament corporations specialized in high-tech equipment and future weapons systems actively on the market, as well as politics, clearly keeping the dangers of networked infrastructure in mind and trying to fight it with measurements as the "Cyberwarfare Defense Centers".

All in all, these points seem to resemble the fact that cyberwar is to be seen as regular war. But what about the other aspects? A cyberwar is not declared and in no way restricted to a certain area. It cannot even be assured that two countrys are fighting this "war" - given the fact that even individuals did already attack important structures as the Pentagon or similar military installations. And there is also no indicated end to such a kind of "war".

Given all these facts, cyberwar does resemble more a kind of asymmetrical warfare or terrorist warfare than an normal war.

But at the same time, we must ask which wars are led today? Even tough former president George W. Bush did call for an "war against terror" - this was none by definition. Traditional warfare, as it was meant in the case of World War I, World War II or even the Franco-German War did disappear over time. Neither the undeclared Vietnam War, nor the "war against terror" were wars by definition, and nevertheless, none would refuse to call Vietnam one.

Computerization and the overall development of humanity and technology has not only changed the face of the world we live in today, but also the face of war. But not the definition of the word itself. Maybe it is time to rewrite it.

References

[1] B. Schneier, "The Threat of Cyberwar," 2010. [Online]. Available: http://www.schneier.com/blog/archives/2010/07/the_threat_of_c.html

[2] Cambridge University Press, "cyber," 2012. [Online]. Available: http://dictionary.cambridge.org/dictionary/british/cyber?q=cyber

[3] ——, "war," 2012. [Online]. Available: http://dictionary.cambridge.org/dictionary/british/war?q=war

[4] Symantec. (2010) Stuxnet Target Configuration. [Online]. Available: http://www.symantec.com/connect/blogs/stuxnet-breakthrough

[5] Wired, "Security Pros Question Deployment of Smart Meters," 2010. [Online]. Available: http://www.wired.com/threatlevel/2010/03/smart-grids-done-smartly/

[6] T. Steuer, "Smart Meters: Ein Security-Albtraum?" 2012.

[7] Wallstreet Journal Online, "Computer Spies Breach Fighter-Jet Project," 2009. [Online]. Available: http://online.wsj.com/article/SB124027491029837401.html#

[8] Attendconference. (2011) RSA Security offers to replace SecurID tokens. [Online]. Available: http://www.attendconference.com/blog/engineering-technology/rsa-security-offers-to-replace-securid-tokens-wsj

[9] Tech News Daily, "Did Chinese Hackers Delay America's Next Fighter Jet?" 2012. [Online]. Available: http://www.technewsdaily.com/7519-chinese-hackers-joint-strike-fighter.html

[10] Wallstreet Journal Online, "Insurgents Hack U.S. Drones," 2009. [Online]. Available: http://online.wsj.com/article/SB126102247889095011.html#

[11] Wired, "Computer Virus Hits U.S. Drone Fleet," 2011. [Online]. Available: http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

[12] ——, "Air Force Insists: Drone Cockpit Virus Just a Nuisance," 2011. [Online]. Available: http://www.wired.com/dangerroom/2011/10/drone-virus-nuisance/

[13] CNet, "Drones can be hijacked via GPS spoofing attack," 2012. [Online]. Available: http://news.cnet.com/8301-1009_3-57464271-83/drones-can-be-hijacked-via-gps-spoofing-attack/

[14] Wired, "Drone Hijacking? Thats Just the Start of GPS Troubles," 2012. [Online]. Available: http://www.wired.com/dangerroom/2012/07/drone-hijacking/

[15] GPS Navi Reviews. (2010) How GPS works. [Online]. Available: http://www.gpsnavireviews.com/how-gps-works/

[16] International Atomic Energy Agency, "Tools for Nuclear Inspection," 2004. [Online]. Available: http://www.iaea.org/Publications/Factsheets/English/inspectors.pdf

[17] SIPRI, "The SIPRI Top 100 arms-producing and military services companies, 2010," 2010. [Online]. Available: http://www.sipri.org/research/armaments/production/Top100
[18] Heise, "Robocop soll die innerkoreanische Grenze schützen," 2007. [Online]. Available: http://www.heise.de/newsticker/meldung/Robocop-soll-die-innerkoreanische-Grenze-schuetzen-138623.html
[19] Human Rights Watch. (2012) Pull the Plug on Killer Robots. [Online]. Available: http://www.youtube.com/watch?v=AlRIcZRoLq8
[20] NATO, "What is Article 5?" 2005. [Online]. Available: http://www.nato.int/terrorism/five.htm
[21] N. Joseph, "Can NATOs cyber defence outfox the Hacktivists," 2012. [Online]. Available: http://we-nato.org/2012/04/24/852/
[22] Defense News, "Japan Takes Action Against Complex Cyber Threats," 2012. [Online]. Available: http://www.defensenews.com/article/20121009/C4ISR01/310090010/Japan-Takes-Action-Against-Complex-Cyber-Threats
[23] Der Spiegel, "Fighting Internet Threats: Germany Arms Itself for Cyber War," 2011. [Online]. Available: http://www.spiegel.de/international/germany/fighting-internet-threats-germany-arms-itself-for-cyber-war-a-768764.html
[24] ——, "Cyberwar: Pentagon verfünffacht seine Netzstreitmacht," 2013. [Online]. Available: http://www.spiegel.de/netzwelt/netzpolitik/us-cyber-command-aufruestung-um-das-fuenffache-a-879990.html
[25] CNet, "Obama signs order outlining emergency Internet control," 2012. [Online]. Available: http://news.cnet.com/8301-1023_3-57469950-93/obama-signs-order-outlining-emergency-internet-control/
[26] Wired, "Report: Egypt Shut Down Net With Big Switch, Not Phone Calls," 2011. [Online]. Available: http://www.wired.com/threatlevel/2011/02/egypt-off-switch/
[27] The Aviationist, "Iran claims it has decoded the U.S. stealthy RQ-170 Drone Intel but provides unsubstantiated evidence to prove it," 2012. [Online]. Available: http://theaviationist.com/2012/04/22/rq170-drone-decoded/