Recent Cyberwar Spectrum and its Analysis

Rabia Aslanoglu, Selma Tekir
Izmir Institute of Technology, Izmir, Turkey
rabiaaslanoglu@iyte.edu.tr
selmatekir@iyte.edu.tr

Abstract: War is an organized, armed, and often prolonged conflict that is carried on between states, nations or other parties. Every war instance includes some basic components like rising conditions, battlespace, weapons, strategy, tactics, and consequences. Recent developments in the information and communication technologies have brought about changes on the nature of war. As a consequence of this change, cyberwar became the new form of war. In this new form, the new battlespace is cyber space and the contemporary weapons are constantly being renovated viruses, worms, trojans, denial-of-service, botnets, and advanced persistent threat.

In this work, we present recent cyberwar spectrum along with its analysis. The spectrum is composed of the Estonia Attack, Georgia Attack, Operation Aurora, and Stuxnet Worm cases. The methodology for analysis is to identify reasons, timeline, effects, responses, and evaluation of each individual case. Moreover, we try to enumerate the fundamental war components for each incident. The analysis results put evidences to the evolution of the weapons into some new forms such as advanced persistent threat. Another outcome of the analysis is that when approaching to the end, confidentiality and integrity attributes of information are being compromised in addition to the availability. Another important observation is that in the last two cases, the responsive actions were not possible due to the lack of the identities of the offending parties. Thus, attribution appears as a significant concern for the modern warfare.

The current sophistication level of the cyber weapons poses critical threats to society. Particularly developed countries that have high dependence on information and communication technologies are potential targets since the safety of the critical infrastructures like; healthcare, oil and gas production, water supply, transportation and telecommunication count on the safety of the computer networks. Being aware of this fact, every nation should attach high priorities to cyber security in his agenda and thus behave proactively.

Keywords: Cyberwar, Estonia Attack, Georgia Attack, Operation Aurora, Stuxnet Worm.

1. Introduction

Among all centuries, a human being starting from his birth somehow got included in a group, community, society or nation. All these group titles, their functions and their legitimacy has changed throughout history; but the thing that remained the same is continual conflicts between different groupings, which conveyed the concept of war.

War is an inevitable fact of humanity. In every war, one recognizes some basic components like rising conditions, battlespace, weapons, strategy, tactics and consequences. Rising condition is growing reasons of conflict; battlespace signifies the realm of war whether it's air, sea, or land; weapon is an army's means of defence or offence; strategy can be stated as a high-level plan in order to achieve a defeat; and tactic is a way of using the appropriate weapons or resources to fulfill a strategy; and finally consequences are the victories or defeats, and effects on the opposing parties. Among these components, weapon is the transforming one by evolving from sword, arrow, spread to gun, rocket, nuclear weapons and medical weapons along the timeline.

In the 21st century, the war concept has experienced a paradigm shift in terms of battlespace and weapon components. Today the new battlespace is cyber space and the contemporary weapons are constantly being renovated viruses, worms, trojans, denial-of-service, botnets etc. The strategy is being adjusted through these weapons to damage core attributes of information security using propaganda, espionage or destruction of critical infrastructures. The addressed security attributes are confidentiality, integrity and availability which is known as CIA triad.

CIA is comprised of three criteria to evaluate information systems security (MU, 2008). The first criterion, confidentiality is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information . A loss of confidentiality is the unauthorized disclosure of information. Integrity is guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information. As for availability, it is ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system (Evan, 2004).

The more primitive cyber attacks were aimed at the availability attribute of information security and left observable symptoms. However, with the evolution of cyberwar weapons, the recent cyber incidents compromised confidentiality and integrity attributes in addition to the availability attribute and rendered themselves hard to recognize.

This study will cover Estonia Attack, Georgia Attack, Operation Aurora and Stuxnet Worm cases to put some evidences to the evolution of weapons of cyber war and their effects to security attributes.

2. Estonia Cyberwar

Estonia is located in the Baltic Region of Northern Europe. It declared its formal independence on the 20th of August 1991 from Soviet Union. With the population of 1,34 million, it is the least populous member of Eurozone and referred as a developed country by United Nations (Wikipedia, 2011a).

Estonia attack is the first known public cyberwar case in terms of its effectiveness. It brought the country's IT infrastructure to a standstill though Estonia was one of the most developed countries in Europe with ubiquitous usage of information and communication technologies in all areas of life. All government organizations in Estonia have used X-Road (Figure 1) to interconnect with each other since 2001 and all citizens have an ID-card which allows them to connect with the goverment organizations and banks (Afrinic-11, 2009).

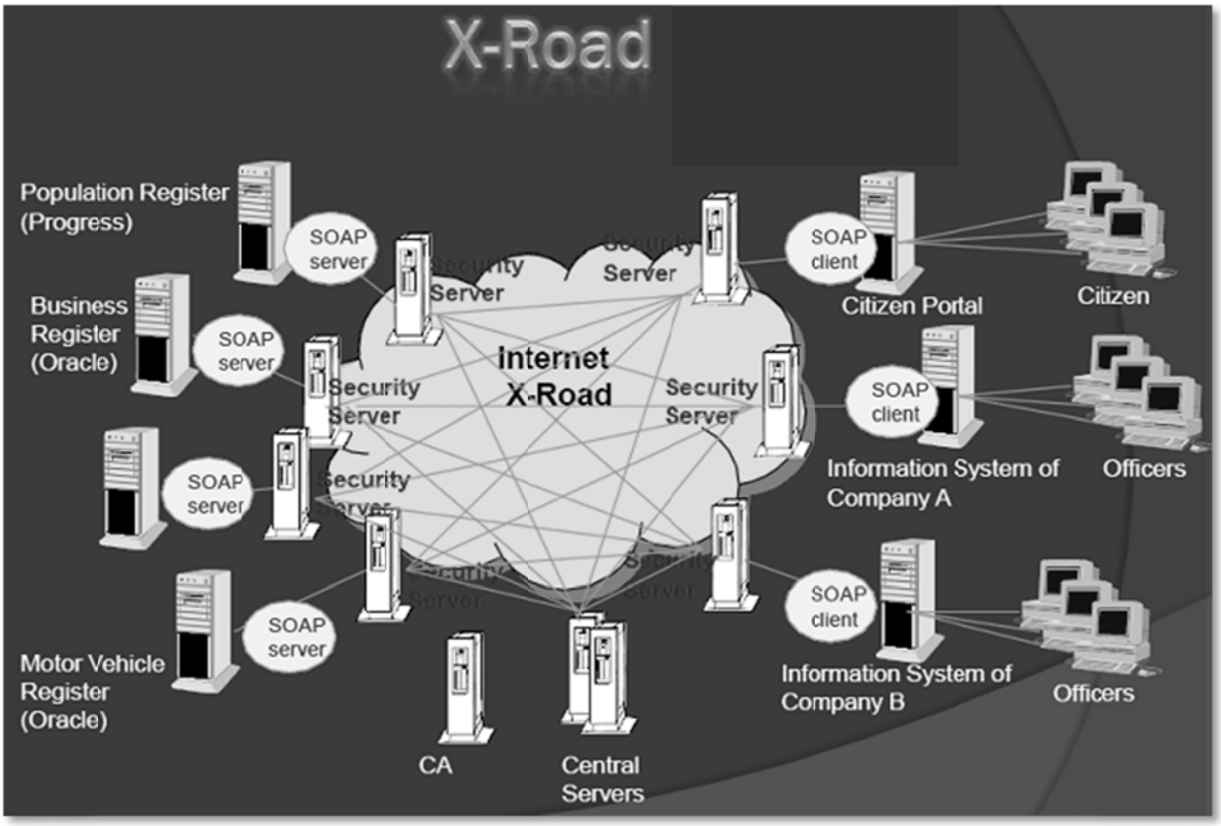

Figure 1: X-Road architecture (Afrinic-11, 2009).

Cyberattacks on Estonia began on April 27th 2007 since the Estonian Government moved a controversial Soviet-era World War II memorial from a square in the capital city of Tallinn to a more secluded location (Traynor, 2007). Protests erupted in Estonia and Russia, where Estonia's Moscow embassy was blockaded (Silverman, 2008).

A series of politically motivated cyber attacks targeting government portals, parliament portal, banks, ministries, newspapers and broadcasters of Estonia hit it and lasted three weeks. Typical attacks were phishing, email spam, web site defacing, syn/ICMP floods, botnets.

In the first wave of attacks, DDoS occurred to Estonia's ISP and governmental websites. Command of ICMP attacks posted to various boards, blogs and chats on Russian Internet. These commands converted into a batch file and uploaded to a web address (Afrinic-11, 2009).

In the second wave, Livejournal users have posted a list of email addresses of Estonia's parliament deputies. These posts were urging users to share the list of emails and caused multiple letters to be sent to the Estonia's deputies with "congratulations of the Victory Day". This action resulted millions of letters being sent and led to mail server mainframes' failure for 2 days.

In the third wave , Estonia's websites were attacked with various tools such as SQL injections (known vulnerabilities in Apache, PHP). Script kiddies were stoked into fervour by President Vladimir Putin's speech (Afrinic-11, 2009).

The attack heavily affected all network infrastructure; leaving damaged routers, changed routing tables, overloaded DNS servers, failed e-mail servers. Estonian Presidency and its Parliament, country's government ministries, political parties, two biggest banks, governmental ISP, telecom companies experienced interoperability problems.

After the attack, Estonia closed down the site under attack to foreign internet addresses and kept the sites only accessible to domestic users. 99% of bogus traffic coming from outside was cut and all ".ru" domain was blocked. Also, bots from DNS servers were identified and blockaded. Estonia's Computer Emergency Response Team (CERT) acted as a coordinating unit, concentrating its efforts on protecting the most vital resources. It persuaded ISPs around the world to blacklist attacking computers which overwhelmed Estonia's bandwith (Afrinic-11, 2009).

The methods used in this attack were not new. However, the country's small size and high reliance on information and communication technologies made the attack a significant threat. As Estonia had an established IT infrastructure, the incident was handled appropriately before the damage was grown. The weapons of this case are phishing, e-mail spam, web site defacing, Syn/ICMP floods, botnets, DDoS which damage availability. The strategy is to test IT infrastructure and make the digital services temporarily down in order to retaliate for the removal of the Soviet-era memorial and prove the Russian power. The consequence is the access failure to the existing information systems in the result of availability disruption (Table 1).

3. Georgia Cyberwar

Georgia is an old Soviet Union member which is located at the crossroads of Western Asia and Eastern Europe with 4,7 million population (Wikipedia, 2011b).

Statistics about the Georgian ICT sector show that Georgia has 7 Internet users per 100 people (UNdata, 2006). Considering the geography of the region, Georgia has few options for Internet connectivity via land routes, namely Turkey, Armenia, Azerbaijan, and Russia. According to some sources, most of Georgia is, in terms of Internet infrastructure, dependent on Russia; more of Georgia's connections to the Internet pass through Russia than any other country, comprising nearly half of Georgia's thirteen links to the worldwide network (Today, 2008).

Conflict which caused the cyber attack against Georgia was started in August 2008 between Russia and Georgia over South Ossetia. On August 7th , Georgian forces launched a surprise attack against separatist forces in South Ossetia who was supported by Russia (Tikk, 2008). On August 8th , Russia responded to Georgia's act by military operations into Georgian territory, which the Georgian authorities viewed as Russia's military aggression against Georgia (MFAG, 2008).

By late August 7th, before the Russian invasion into Georgia commenced, cyber attacks were already being launched against a large number of Georgian governmental websites(Tikk, 2008), making it among the first cases in which an international political and military conflict was accompanied by a coordinated cyber offensive. On the August 8th, the President of Georgia, Mikheil Saakashvili, informed the international community of having begun mobilisation, and on August 9th, 2008, Georgia imposed a "state of war" (Saakashvili, 2008).

The methods of these attacks primarily included defacement of public websites containing Mikheil Saakashvili and the National Bank; and launch of DDoS attacks against government sites, important media sites, financial institutions (Tikk, 2008).

In this cyber incident, numerous targets and methods are similar to attacks used in Estonia. Several Russian blogs, forums, and websites spread a Microsoft Windows batch script that was designed to attack Georgian websites. Instructions of these downloadable scripts to ping flood Georgian government websites and lists of vulnerable Georgian sites were distributed on Russian websites and message boards. Emails of Georgian politicians were subjected to targeted attacks and spamming. Georgia has two main players on the Georgian Internet Access and services market; United Telecom and Caucasus Network. United Telecom of Georgia router was unavailable and incapable of providing service for several days. Caucasus Network was flooded with excessive queries. On August 9th, the National Bank of Georgia ordered all banks to stop offering electronic services.

After the attack, some of the damaged websites remained online and did not really make any changes to defend themselves. A few of them temporarily changed their IP addresses to loop back to the originating network in an attempt to thwart the attacks. A few others also changed hosts. The websites of the Ministry of Defence and the President were relocated to Tulip Systems, Inc., located in Atlanta, Georgia, USA, and the website of the Ministry of Foreign Affairs was moved to an Estonian server. The Office of the President of Poland provided their website for dissemination of information and helped to get Internet access for Georgia's government after breakdowns of Georgian local servers caused by cyber attacks. CERT Poland analyzed IP data and sent out abuse messages, while CERT France helped with collecting log files. Security specialists from CERT Estonia also visited Georgia in order to assist the local CERT by providing their know-how and experience. As it's apparent from the examples, international cooperation and assistance were offered, international awareness was raised, and media attention was drawn (Tikk, 2008).

Although the methods used in the attack were the same as Estonia case, the density of the damage was higher than it. Georgia couldn't manage the incident properly due to unsound IT infrastructure and high dependency on neighboring countries for internet connectivity. After all the most important disruption is that the timing of the cyber incidents coincided with the physical damages caused by the ongoing armed conflict and this situation resulted in discredit to the authority.

The weapons of this case are DoS, DDoS, web site defecement, TCP SYN floods, TSC RST flood phishing, e-mail spam which target availability attribute as was in Estonia cyber case but the intensity of the attacks was higher than Estonia. The strategy is to exploit unsound IT infrastructure in order to support the military conflict in cyberspace. All these heavy consequences occurred due to availability disruption (Table 1).

4. Operation Aurora

On January 12th, 2010 Google publicly disclosed that they were under a highly sophisticated and targeted attack on their corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. It claimed that the attackers were interested in accessing Gmail accounts of Chinese dissidents, as well. Google was not the only victim of this attack; at least twenty other large companies from a wide range of business including; the internet, finance, technology, media and chemical sectors have been similarly targeted (Drummond, 2010).

In Estonian and Georgian cases; cyber attacks occurred against users and after a while, they became aware. However, Aurora attack's landscape is against software; which exploited a browser vulnerability and occurred silently without user awareness. The attack leveraged a previously unknown vulnerability in Internet Explorer to compromise systems at Google, Adobe and more than 30 large companies. According to McAfee, primary goal of the attack was to gain access to and potentially modify source code repositories at these high tech, security and defense contractor companies (Kurtz, 2010). It completed its attack in six steps (McAfee, 2010):

- A targeted user received a link in email or instant message from a "trusted" source.
- The user clicked on the link which caused them to visit a website hosted in Taiwan that also contained a malicious JavaScript payload.
- The user's browser downloaded and executed the malicious JavaScript, which included a zero-day Internet Explorer (IE) exploit.
- The exploit downloaded a binary disguised as an image from Taiwan servers and executed the malicious payload.
- The payload set up a backdoor and connected to command and control servers in Taiwan.
- As a result, attackers had complete access to internal systems. They targeted sources of intellectual property, including software configuration management (SCM) systems accessible by the compromised system. The compromised system could also be leveraged to further penetrate the network.

Aurora employed an advanced persistent threat (APT) technique that proved extremely successful in targeting, exploiting, accessing, and exfiltrating highly valuable intellectual property from its victims (McAfee, 2010). APT is named by the United States Air Force analysts in 2006 in order to facilitate discussion of intrusion activities with their uncleared civilian counterparts (Daly, 2009).

Advanced means the adversary is conversant with computer intrusion tools and techniques and is capable of developing custom exploits (Daly, 2009).

In Aurora case, attackers gained initial access to the victim's network with a targeted spear phishing attack against the company. Several employees of the victim companies received an email that appeared to be from someone they trusted. However, the email contained a link to a Taiwanese website that hosted malicious JavaScript. The malware, in turn, exploited IE vulnerability. The exploit triggers when IE attempts to access memory that has been partially freed. In short, sophisticated attackers fulfilled the *advanced* criterion of APT (Binde, 2011).

Persistent means the adversary intends to accomplish a mission. They receive directives and work towards specific goals (Daly, 2009).

In Aurora case, after gaining a foothold in the victim companies, the attackers employed the exploited workstations to compromise other internal resources. The attackers then targeted SCM systems and exfiltrated source code to the attacker's command and control servers which was with innocuous-sounding domain names such as homelinux.org, ourhobby.com and servebeer.com (Lelli, 2010). In January 2010, Google was the first to publicly disclose loss of intellectual property. The attackers accomplished a specific mission meeting the *persistence* criterion of APT (Binde, 2011).

Threat means the adversary is organized, funded and motivated. Furthermore, there are objectives that may be political, economic (e.g., theft of intellectual property), technical or military (identification of weaknesses) (Daly, 2009).

The attacks traced back to two Chinese schools, Shanghai Jiaotong University and Lanxiang Vocational School. Jiatong hosts one of the top computer science programs in China. In 2010, it beat Stanford University in an international programming competition sponsored by IBM. Lanxiang is a large vocational school established with military support, training some computer scientists for the military. The school is operated by a company with close ties to Baidu, a strong Chinese competitor to Google. Sources within the schools denied organizational involvement in the attacks (Markoff, 2010). The adversaries, whatever their actual identities, demonstrated high motivation, were adequately funded, and were part of a structured organization and this meets the *threat* criterion (Binde, 2011).

APT is the weapon of this attack and the strategy is to exploit internet vulnerabilities in order to steal intellectual property and retaliate to Chinese human right activists by spying. After the incident, modification of source code in repositories, theft of trade secrets and unauthorized access to e-mails of Chinese human right activists prove the disruption of availability, confidentiality and integrity respectively (Table 1).

5. Stuxnet Worm

Stuxnet increased attack sophistication level when it discovered in June, 2010. Months later Iran confirmed that centrifuges for uranium enrichment production at Natanz were affected and potentially damaged by it. Stuxnet was unique and did not follow traditional Web threat patterns and tactics (Clare, 2011). Also, it has apparently infected over 60,000 computers, more than half of them in Iran; other countries affected include India, Indonesia, China, Azerbaijan, South Korea, Malaysia, the United States, the United Kingdom, Australia, Finland and Germany. The virus continues to spread and infect computer systems via the Internet, although its power to do damage is now limited by the availability of effective antidotes, and a built-in expiration date of 24 June 2012 (Farwell, 2011).

Bruce Schneier's analysis on Forbes.com suggests air-gapped Windows systems were infected by the Stuxnet worm via USB, that four unpublished and highly valuable zero-day vulnerabilities were exploited, and that Stuxnet looks for a particular model of a Programmable Logic Controller (PLC) manufactured by Siemens, and its related controller software. Stuxnet installs its own driver in Windows using stolen certificates to legitimize itself, and checks back with two control servers for updates. It uses a peer-to-peer update scheme when it encounters itself, so the most current version is always utilized (Clare, 2011).

This was an unprecedented sophisticated attack that would have wide implications for future industrial systems because it has broken down common beliefs about control systems security on industrial infrastructures. Before the Stuxnet, there was an image that control systems were safe as far as new USB was used for data exchange and internet was not connected; and a virus could be monitored thanks to abnormal behaviours of related computer (Miyachi, 2011). Additionally, it occurred at an extremely critical time as industrial systems move towards the adoption of Internet based technologies and architectures (Karnouskos, 2011b). Its main target is industrial control systems with the goal of modifying the code running in PLCs in order to make them deviate from their expected behavior (Matrosov, 2010). This deviation would be small and only noticeable over a longer period of time. In parallel great effort was put by the Stuxnet creators in hiding those changes from the operators, even imitating “legitimate” data. To increase the success rate, a vast majority of security holes and tools was used such as rootkits, antivirus tricking, zero-day exploits, network discovery and peer-to-peer updates, process injection etc. Many of these are common on modern PCs but the sophistication of the attack was unprecedentedly well-planned and highly customized for specific industrial systems. It is believed that the development of such a highly sophisticated worm was a joint-effort with experts from different specializations and a huge investment in time and cost (Karnouskos, 2011a).

All of them make Stuxnet another Advanced Persistent Threat. The evidences are stated below:

Advanced: The original infection of the Windows computer may be done via simply plugging in a USB flash drive or from internal network if an infected machine exists. It uses stolen certificates in order to legitimize itself and then installs its own driver in Windows. When it encounters itself, it uses peer-to-peer update scheme.

Persistent: The target was solely Siemens SCADA systems targeting very specific industrial processes. Stuxnet infects project files of Siemens WinCC/PC S7 SCADA control software and intercepts the communication between the WinCC running in Windows and the attached PLC devices when the two are connected via a data cable (known as “man-in-the-middle” attack). It focused on identifying specific slave variable frequency drives attached to the Siemens S7-300 system. Furthermore it has been reported that it would only attack specific provider of those PLC systems. However in order to have a more specialized target, it monitors the frequency of the attached motors, and only attacks systems that spin between a specific range. Then it installs malware on the PLC that monitors the Profibus of the system and under certain conditions it periodically modifies that frequency, which results in that the connected motors change their rotational speed. Additionally it has installed the first known industrial rootkit which fakes industrial process control sensor signals, hence no alarms or shutdown is done due to abnormal behavior. This slowly deviating behavior in combination with the projection of “legitimate” data results in difficulty to assess what is malfunctioning and to pinpoint the faults before it is too late (Karnouskos, 2011a).

Threat: It is the first purpose-built worm designed to attack PLC, industrial control systems that help run critical infrastructure environments. As such, it can be hypothesized that Stuxnet was designed purely to attack PLCs and cause damage to the infrastructure they operate and, ultimately, to the people and organizations that depend on that infrastructure. Stuxnet is clearly an example of a stealthy worm developed by an adversary that spent a great deal of time and money on research and development. While the origins are still unknown, many experts feel that it was likely developed by a nation-state with nefarious intent driven by political rather than economic motivations (McAfee, 2011).

Stuxnet’s design and architecture are not domain specific; it is a tool for APT. Hence with some modifications it could be tailored as a platform for attacking other systems e.g. in the automobile or power plants. Monitoring and control systems such as SCADA/DCS are responsible for managing critical infrastructures operate in these environments. Its highly sophisticated actions may prevent detection until it is too late (Karnouskos, 2011a). For Iran case, the strategy is to exploit control systems vulnerabilities in order to damage country reputation and avoid attribution. As a result of the attack Iran’s centrifuges were affected and potentially damaged and over 60,000 computers from other countries were infected. These happenings are indicators of availability, integrity and confidentiality disruption.

By the appearance of this worm, cyber security has become a high-priority item in agendas. Barack OBAMA’s the following statement supports this argument: “Cybersecurity is a matter of public safety and national security. We count on computer networks to deliver our oil and gas, our power and our water, public transportation and air traffic control.” (Obama, 2009). So high dependence on information and communication technology brings about new hidden weapons pointed at well-developed countries by exploiting their critical infrastructures. Stuxnet is the peak point of cyberweapons came.

6. Discussion

In Table 1, each war case is examined in terms of the associated war components. Considering the contents of the table and thus recognizing the tactical and weaponry differences, the examined war incidents can be divided into two groups: Estonia-Georgia and Aurora-Stuxnet respectively. In the former group, the main tactic is propaganda and the weapons are traditional cyber threats while in the latter, espionage is the common tactic and the weapons are referred as Advanced Persistent Threat.

Both Estonia and Georgia cases stand on political disputes. Although the weapons and consequences are partially similar to each other, Georgia experiences higher damage because of its unsound IT infrastructure. These cases are references of disruption in which masses of attack are traceable and familiar in landscape.

Commercial competition lies behind the Aurora case. It heats up the attack sophistication level by occurring silently without user awareness. Succeeding Aurora, Stuxnet is the peak point for cyberweapons thanks to its unprecedented attack combination and sophistication. Particularly this unique characteristic renders Stuxnet resistant to attribution. In both Aurora and Stuxnet cases, offensive parties were conversant with computer intrusion tools and techniques to accomplish a mission receiving directives, organized, funded, motivated for economic and political objectives exhibiting an Advanced Persistent Threat pattern.

Table 1: General Picture of the Cases

War	*Estonia 2007*	*Georgia 2008*	*Aurora 2009*	*Stuxnet 2010*

Rising Conditions	Political; elocation of a Soviet war memorial.	Political; occurrance of Georgian surprise attack against separatist forces in South Ossetia.	Global competition, political; Google's internet domination and Chinese human right activists' activities.	Political Keeping Iran's Uranium enrichment under control.
Battlespace	Cyberspace	Land & Cyberspace	Cyberspace	Cyberspace
Weapons	DoS and DDoS, defacement, e-mail and comment spam, Some targeted hacks using exploits/SQL injections.	DoS and DDoS, defacement, TCP SYN floods, TCP RST flood.	Advanced Persistent Threat.	Advanced Persistent Threat.
Goal	Retaliate for the removal of the Soviet-era memorial, prove the Russian power.	Support the military conflict in cyberspace.	Steal intellectual property, retaliate to Chinese human right activists.	Damage reputation, avoid attribution.
Strategy	Test IT infrastructure, make the digital services temporarily down.	Exploit unsound IT infrastructure.	Exploit internet vulnerabilities.	Exploit control systems vulnerabilities.
Tactics	Propaganda.	Propaganda.	Espionage.	Espionage.
Consequences	The disruption of access to related web sites and use of information of e-mail servers, bank system and telecom system occurred. (Availability disruption).	The disruption of use of information of e-mail servers, bank system and telecom system government sites, important media sites, financial institutions occurred. Higher intensity attacks compared to Estonia. (Availability disruption).	Modify source code in repositories, steal trade secrets and read e-mails of chinese human right activists (Availability, confidentiality and integrity disruption).	Iran's centrifuges were affected and potentially damaged, infected over 60,000 computers from other countries,too. (Availability, confidentiality and integrity disruption).

7. Conclusion

War is an inevitable fact of humanity. In the 21st century, the war concept has experienced a paradigm shift in terms of battlespace and weapon components. Today the new battlespace is cyber space and the contemporary weapons are constantly being renovated viruses, worms, trojans, denial-of service, botnets etc. Its current strategy is being adjusted through these weapons to damage core attributes of information security using propaganda, espionage or destruction of critical infrastructures.

This study aims to cover Estonia Attack, Georgia Attack, Operation Aurora and Stuxnet Worm cases to put some evidences to the evolution of weapons of cyber war and their effects to security attributes. The presented cyber attack cases are the important instances of the past five years. Most of the cyber weapons are not new in information technology but their unprecedented combination and sophistication have threatened well-developed countries in the matter of exploiting.

References

Afrinic-11 (2009) "Estonia Cyber Attacks 2007", [online], http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf.

Binde B., McRee R. and O'Connor T. J. (2011) Assessing Outbound Traffic to Uncover Advenced Persistent Threat, SANS Technology Institute.

Clare, T. (2011) "2011 WebSecurity Report", *White Paper*, Blue Coat.

Daly, M. K. (2009) "The Advanced Persistent Threat", *23rd Large Installation System Administration Conference.*

Drummond, D. (2010) "A new approch to China", [Online], *The Official Google Blog*, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

Evan, D. L., Bomb, P. J. and Bement A. L. (2004) *Standards for Security Categorization of Federal Information and Information Systems*, Department of Commerce, Federal Information Processing Standards Publication: National Institute of Standards and Technology.

Farwell, J. P. and Rohozinski, R. (2011) "Stuxnet and the Future of Cyber War", *Survival: Global Politics and Strategy,* 23-41.

Karnouskos, S. (2011a) "Stuxnet worm impact on industrial cyber-physical system security", *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*, 4490-4494.

Karnouskos, S. and Colombo, A. W. (2011b) "Architecting the next generation of service-based SCADA/DCS system of systems", *IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society*, 359-364.

Kurtz, G. (2010) Operation "Aurora" Hit Google, Others, [Online], *McAfee Blog* http://siblog.mcafee.com/cto/operation-%E2%80%9Caurora%E2%80%9D-hit-google-others/.

Lelli, A. (2010) "Trojan.hydraq technical details", [Online], Symantec Corporation: Symantec Corporation, http://www.symantec.com/security_response/writeup.jsp?docid=2010-011114-1830-99&tabid=2.

Markoff, J. and Barboza D. (2010) "2 china schools said to be tied to online attacks", [online] *The New York Times*, http://www.nytimes.com/2010/02/19/technology/19china.html?_r=1.

Matrosov, A., Rodionov, E., Harley, D. and Malcho J. (2010) "Stuxnet under the microscope", *Technical Report,* ESET.

McAfee (2011) "Advanced Persistant Threat", *Solution Brief.*

McAfee (2010) "Protecting Your Critical Assets, Lessons Learned from Operation Aurora", *White Paper*, McAfee Foundstone Professional Services.

MFAG (2008) "Information for press", Press and Information Department, [press released], 8 August 2008, http://www.mfa.gov.ge/index.php?lang_id=ENG&sec_id=461&info_id=7193&date=2008-0808&new_month=08&new_year=2008.

MU (2008) "Confidentiality, Integrity and Availability (CIA)", [Online], University of Miami, http://it.med.miami.edu/x904.xml.

Miyachi, T., Narita, H., Yamada, H. and Furuta, H. (2011) "Myth and reality on control system security revealed by Stuxnet", SICE Annual Conference, pp 1537-1540.

Obama, B. (2009) "Remarks by the Presidet on securing our notion's cyber infrastructure", The White House, [press released], 29 May 2009, www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

Saakashvili, M. (2008) "News", Press Office of The President of Georgia, [press released], 8 Sept 2008, http://www.president.gov.ge/en/PressOffice/News?2273.

Silverman, J. (2008) "Cyber Attacks in Estonia", [Online], HowStuffWorks, http://computer.howstuffworks.com/die-hard-hacker1.htm.

Tikk E., Kaska K., Rünnimeri K., Kert M., Taliharm A. and Vihul L. (2008) "Cyber Attacks Against Georgia:Legal Lessons Identified", Nato, Cooperative Cyber Defence Centre of Excellence.

Today, S. (2008) "Georgia, Russia: The Cyberwarfare Angle" [Online], www.stratfor.com/analysis/georgia_russia_cyberwarfare_angle.

Traynor, I. (2007) "Russia accused of unleashing cyberwar to disable Estonia", [online], The Guardian, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

UNdata (2006) "Internet users per 100 population, 2006" [online], http://data.un.org/Data.aspx?d=MDG&f=seriesRowID:605.

Wikipedia (2011a) "Estonia" [Online], http://en.wikipedia.org/wiki/Estonia, [accessed on 02/01/12].

Wikipedia (2011b) "Georgia" [Online], http://en.wikipedia.org/wiki/Georgia, [accessed on 02/01/12].