International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:8, No:4, 2014

Active Cyber Defense within the Concept of NATO's Protection of Critical Infrastructures

Serkan Yağlı, Selçuk Dal

***Abstract*—**Cyber attacks pose a serious threat to all states. Therefore, states constantly seek for various methods to encounter those threats. In addition, recent changes in the nature of cyber attacks and their more complicated methods have created a new concept: active cyber defense (ACD). This article tries to answer firstly why ACD is important to NATO and find out the viewpoint of NATO towards ACD. Secondly, infrastructure protection is essential to cyber defense. Critical infrastructure protection with ACD means is even more important. It is assumed that by implementing active cyber defense, NATO may not only be able to repel the attacks but also be deterrent. Hence, the use of ACD has a direct positive effect in all international organizations' future including NATO.

***Keywords*—**Active cyber defense, advanced persistent treat, critical infrastructure, NATO.

I. Introduction

TODAY, information and communication technologies are increasingly embedded in all dimensions of our daily lives. Critical infrastructure (CI) of homeland security, transportation, communication, finance, etc. are extensively digitalized and heavily rely on communication technologies. It is vital to keep these systems untouched and secure. Recent cyber attacks have gotten more complex and brought about great security concerns for states. Passive countermeasures look incompetent to fight against these advanced cyber threats. Perception of new sophisticated cyber threats urged states to resort to active cyber defense methods. After 2007 Estonia cyber attacks, NATO embarked studies on developing new cyber strategies. However, it is still widely discussed that whether these efforts will be effective enough to fight in such a changing and elusive cyber-threat environment.

This article aims to expand the discussion mentioned above. First, Advanced Persistent Threat (APT) and active cyber defense (ACD) will be explained and then, importance of ACD and legality of ACD will argued for a common understanding. Second, the definition of critical infrastructure, legal issues of critical infrastructure protection (CIP) will be discussed. Finally, NATO's point of view for CIP will be explained, NATO's cyber defense capabilities will be scrutinized and the question of "what kind of ACD capabilities should NATO develop to overcome advanced cyber threats" will be discussed.

S. Yağlı is with Turkish War Academy, Istanbul, CO 34200 Turkey (phone: +90-553-3212871; e-mail: serkanyagli2004@ gmail.com).

S. Dal is with Turkish War Academy, Istanbul, CO 34200 Turkey (phone: +90-506-3076959; e-mail: selcuk2001@ gmail.com).

II. Active Cyber Defense

Recent cyber attacks have been significantly different from the previous ones in terms of structure and aim. By looking at the attacks it can be deduced that from now on, cyber attacks will be more sophisticated. The adversaries will no longer be the simple hackers, rather, they will be well-organized criminal groups or states, and they will attain their goals by using advanced tools and well-designed techniques. For this reason advanced cyber attacks pose great risks to the countries' national securities [1].

"Advanced Persistent Threat" was first stated by the U.S. Air Force to describe those sophisticated cyber attacks against specific targets in a long period of time [2]. The term describes a particular attack that aims to steal intellectual information or to cause a specific damage to the states or organizations. After deploying into the network, these intrusions stay for a significant period of time, evade conventional firewall and anti-virus capabilities, and enable adversaries to gather crucial information [3].

The general nature of APT has two characteristics. First, the attack has a specific aim such as stealing an intellectual property or causing certain damage to the system. Second, adversaries conduct the cyber attack according to the unique characteristics of that organization, usually by spending great efforts and money.

When we think about the issues mentioned above, we reach two conclusions: First, if an organization has valuable information, it means that it might be exposed to a cyber attack via APT techniques. Second, being exposed to cyber attacks is directly related to the amount of organization's valuable information, which means the more an organization has valuable information the more it will be exposed to cyber attacks [4].

One of the most sophisticated cyber attacks, "Red October", was carried out against diplomatic and governmental agencies in various countries. According to Kaspersky Lab's analysis report, Red October, called also "Rocra" was an advanced cyber attack that had stayed five years in the systems before targeting the government agencies [5]. As it is seen, today's traditional cyber defense options - known also as passive cyber defense applications- do no longer have the ability to prevent the advanced cyber attacks or APTs. Hence these examples bring out a concept called active cyber defense (ACD). It is a term that describes a range of actions to respond to attacks with offensive options. It is estimated that by implementing such ACD techniques, organizations not only stop the cyber attack but also are able to detect the attacker and get back the stolen information as well.

Current cyber attacks are much more sophisticated compared to that of the past. Therefore, active cyber defense has become even more important for nations, governments and private sectors. In addition, the adversary may be not only a hacker but also companies, as well as states.

A. The Necessity of Active Cyber Defense

The head of U.S. Cyber Command (USCYBERCOM), General Keith Alexander said in a speech at the InfoWarCon 2011 conference "waiting and then reacting to cyber intrusions as what we did in the past is no longer enough", and he emphasized the worth of technology that has been stolen from the companies is about 1 Billion US $. So, he expressed that in order to prevent and respond to these threats, active cyber defense approach was urgent [6].

Advanced cyber intrusions are comprised of several phases which enable the adversaries attain their goals. An advanced cyber attack comprises of three steps.

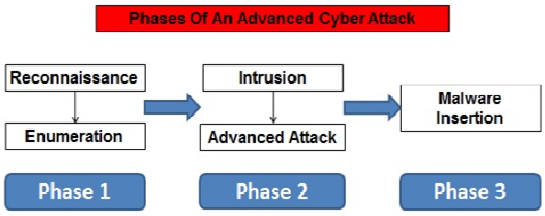

Fig. 1 Phases of an advanced cyber attack

First step is the reconnaissance and enumeration. In this phase, attacker tries to gather information about the network. After reconnaissance, he confidentially finds out the system's vulnerabilities at the enumeration phase. Second step is the intrusion and advanced attack. In this phase, attacker learns about system's vulnerabilities and he leverages of it to penetrate into the networks. Malware insertion is the last step of an advanced attack in which the attacker inserts the malware and exploits it for his particular purpose [7].

Most of the recent cyber attacks that have been carried out can be categorized as advanced cyber attacks. For this reason, it is concluded only active cyber defense options can respond effectively against such cyber attacks. In addition, ACD techniques can deter potential attackers and prevent them. While passive cyber defense can only stop the cyber attack, ACD is able to go beyond stopping the attack by finding the attacker and getting the stolen information back. But this does not mean that ACD techniques can easily be applied, since it is not quite clear that benefits will outweigh the risks [8]. Especially the legality of implementing ACD is under great controversy.

B. Legality of the Active Cyber Defense

Today, technically, active cyber defense options are feasible. Yet, it is not clear whether they are legal. For this reason most of the companies and organizations are hesitant about applying ACD techniques whenever they are exposed to a cyber attack.

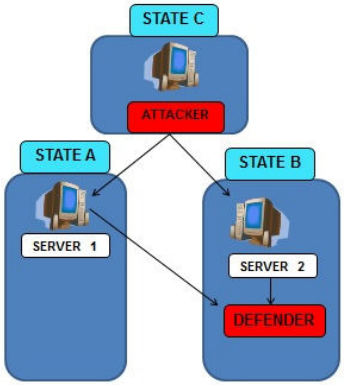

Fig. 2 A Scenario on determining the legality of ACD

In the Fig. 2 we are going to evaluate the legal procedure of ACD in a scenario. According to the scenario there are three states; the attacker is living in the state C and he is able to conduct a cyber attack from servers in State A or B to an organization in State B by using his computer. The defender who has been exposed to the attack in the State B applies the ACD techniques and tries to detect the attacker and try to get the stolen information.

By applying these options, defendant gains access to the servers in other states or another organization in its own country. At this point, we come to a situation that brings out so many questions such as "does defendant has the right to access to the Server 1 or 2 without authorization?" or "what happens when the defendant who gains access to the other servers sees any information that he is unauthorized to see?" "How does the legal procedure function if the attack comes from inside or outside the country?" "When will it violate Computer Fraud and Abuse Act (CFFA) of 1984 or what would happen if the actions made by defendant violate the national law even if it does not violate the CFFA [9]?"

As we see above, the legal procedure of the ACD is very controversial. Using active cyber defense options brings out a controversial situation particularly because of the unanswered questions listed above. Nations all over the world first need to have a clarification on the legal issues of counteracting a cyber attack by ACD means.

III. Critical Infrastructures

Internet has been an indispensable part of our lives recently. Because of the fact that internet is in every sphere of daily life, critical infrastructures such as energy, transportation, information and communication technologies have become vulnerable to sophisticated cyber attacks such as Ddos and Botnet methods. The increase in advanced cyber attacks makes it impossible to solve the problem at individual and institutional levels, and requires agencies to deal with it at national and international level in a comprehensive manner.

In recent years it has been controversial which infrastructure should be called 'critical' and what they are. Due to this controversy, a common definition has not been compromised yet. While some countries define it focusing on

security considerations, some others describe it by emphasizing on human factors.

The critical infrastructures can be defined as; "A cluster of networks, entities, systems and structures that could damage the sustainability of social order and/or public service when they cease to fulfill their functions partially or completely" [10].

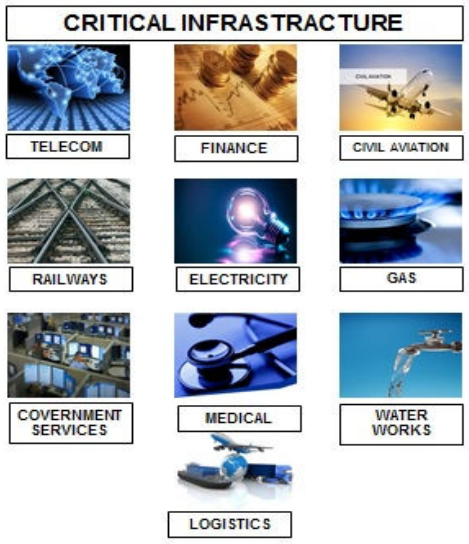

Fig. 3 Critical Infrastructures

Even though it depends on the determined definition of critical infrastructure, in general, CIs are comprised of 10 sectors. These are; telecommunication, finance, civil aviation, railways, electricity, gas, governmental/administrative services, medical services, water works, and logistics [11].

A. Legal Issues of Critical Infrastructure Protection (CIP)

The legal issue of CIP differs from one country to another. However, the legislations of CIP that come to prominence are the Home Land Security Act dated 2002 [12] in US and the EU Commission report about critical infrastructure protection in the fight against terrorism.

With the Homeland Security Act in US, the Department of Homeland Security (DHS) was established. According to this act, DHS undertakes responsibility when a terrorist attack or a natural disaster occurs, and also is the coordinator in planning the CIP against cyber attacks.

The main arrangement about CIP is Homeland Security Presidential Directive / HSPD-7 dates back to 2003. The purpose of this directive is to establish a liability to the governmental organizations of the United States for protecting critical infrastructure and key resources from terrorist attacks [13].

The EU report 'Critical Infrastructure Protection in the Fight Against Terrorism'- the main legislation in EU about CIP- explains what the critical infrastructures are, and what will happen in case any of those critical infrastructures are exposed to a cyber attack. [14]. In addition to this report, studies to establish the communication on a 'European Program for Critical Infrastructure Protection' (EPCIP) have started. According to this program, EU will share responsibilities between the EU and its members. Besides, The Critical Infrastructure Warning Information Network (CIWIN) will be set up in order to help EPCIP in some issues [15].

In protecting critical infrastructure, NATO has broadcast a committee report in 2007 annual session, named "Protection of Critical Infrastructures". According to committee report, NATO would establish four phases for the protection of critical infrastructure; first one is to define what is considered as critical infrastructure, and second one is to identify those infrastructures that fit the definition; then in the third phase, to assess the risk those infrastructures face and identify security gaps; and finally, define and implement appropriate protection measures to reduce this risk [16].

Although several NATO members seem skeptical about the NATO's role in CIP, most of them generally encourage NATO in CIP. Yet, all members of NATO think that CIP remains primarily a national responsibility.

There are two main reasons for that. First, every member state has its own interests; therefore, it is understandable that a member may be unwilling to cooperate without knowing who the attacker is. Secondly, as seen in Estonia example, a member state can be afraid of being exposed to cyber attack in case of helping the victim member. As a result, it may choose not to cooperate. By taking these considerations into account, members have a propensity to defer the attacks on their own and protect the critical infrastructures accordingly. It seems true that NATO is trying to do its best in terms of CIP and cyber defense. However, until the second large-scale attack – like Estonia example- to a member state, it is hard to predict whether NATO will be able to achieve cooperation on cyber defense, especially on CIP.

In conclusion, critical infrastructure protection is vital to cyber defense and NATO is well aware of this. Hence, it is trying to take necessary steps to accomplish an effective CIP. Yet, there are still some setbacks on the table that hinders successful cooperation. For a fruitful CIP, it is considered that NATO should define what critical infrastructure is, identify critical infrastructures, assess the risk that critical infrastructures are exposed to, and take relevant measures to defeat the risks. Moreover, NATO and EU have to cooperate together in responding to cyber threats rather than leaving the members on their own.

IV. NATO and Cyber Defense

In order to have the capability of cyber defense, NATO first decided to build up an organization by using NATO resources in Prague summit in 2002 [17].

In accordance with the summit decisions, a lot of effort has been put forward to enhance NATO cyber defense capabilities since then. Most important of these was the NATO Computer Incident Response Capability (NCIRC) program. According to NATO cyber defense program a three-phase course of action plan was adopted:

1) (2003-2006): Enabling NCIRC with initial operating capabilities.
2) (2006-2012): Developing computer security capabilities and making NCIRC completely operable.
3) (2012-…): Realizing comprehensive cyber defense solutions focusing on legal issues [18].

In 2006 Riga Summit cyber attacks were deemed among asymmetric threats. [19] After the Estonia cyber attack, NATO made some noteworthy progress as to its cyber defense capabilities. First, The Cooperative Cyber Defense Center of Excellence (CCD CoE) [20] was created in 2008 to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defense by virtue of education, research and development, lessons learned and consultation [21]. The main tasks of CCD CoE are [22]; providing cyber-related doctrines and concepts for the Alliance, hosting and conducting training workshops, courses, and exercises for NATO member states, conducting research and development activities, studying past or ongoing attacks to draw up lessons learned, and providing advice, if asked, during ongoing attacks.

Second, a Cyber Defense Management Authority (CDMA) was established in October 2008. Unlike the CCD CoE, an intellectual platform and forum, the CDMA's mission was to centralize cyber defense operational capabilities across the Alliance [23].

Besides CCD CoE and CDMA, the NATO Communications and Information Systems Services Agency (NCSA) is responsible for protecting its communication systems. The four primary tasks of NCSA are [24];

1) CIS support to NATO operations;
2) CIS support to NATO exercises;
3) CIS support to NATO's major headquarters;
4) Support for new CIS systems and projects.

Further, Computer Incident Response Capability (NCIRC) was established to evaluate security of NATO's networks, detect and respond to incidents when they happen [25]. "NCIRC experts are meant to help system administrators to block attacks, limit the damage and repair software errors (so-called vulnerabilities), which make attacks possible" [26]. NATO cyber defense functional structure is shown in Fig. 4 [27].

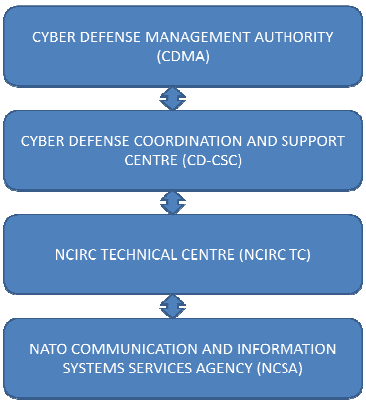

Fig. 4 NATO Cyber Defense Functional Structure

In this structure, CDMA is the sole authority in terms of cyber defense throughout NATO; hence it is responsible of coordination and initiation of any effort for rapid and effective cyber defense. However, NATO's cyber defense actions among members and external organizations take place in CD-CSC. On the other hand, NATO's most important technical capability-NCIRC TC- is responsible for developing, implementing and maintaining cyber defense services.

It can be said that NATO's efforts regarding cyber defense after 2008 improved remarkably. However, it clearly seems that organizations mentioned above are not going to be able to respond effectively enough to an advanced cyber attack towards critical infrastructures. First of all, this is because there is not a common understanding about the critical infrastructures, let alone protecting them together. One member's critical infrastructure is another's luxury. Secondly, due to the attribution problems and high risks of being exposed to cyber attacks, nations usually are reluctant to help other states. Therefore, each member has a general tendency of protecting the critical infrastructures on their own. However, NATO did a lot of things to create a partnership through cyber defense and it is getting better.

Another issue in terms of CIP is the methods used. Since cyber attacks are becoming more advanced and complicated, it may not be enough to stop the attack immediately. Victim should be able to follow the attacker and get back the stolen information at last. However, easier said than done! So, only by implementing active cyber defense means may this be feasible. But, ACD brings out some controversial issues as well. Is it really legal for one to implement ACD techniques? For whom? In what circumstances? To what degree? What if the attacker cannot be identified thoroughly? Similar questions can be posed easily. The point is; there is not a clear legal basis for ACD, yet.

In addition to legality problem of the ACD, there is also cooperation problem. While implementing ACD is difficult enough to apply, implementing ACD as an international organization –in this case NATO- is even more challenging. That requires a lot of coordination and team work. Besides, when carried out in an international organization and in NATO, being able to take risk is essential in ACD since every member state will be exposed to cyber threats once it decides to cooperate.

To our opinion, this highly skilled, coordination requiring abilities can be acquired in terms of CIP by ACD under NATO framework by promoting "mutual cyber trust". One way to do this may be to exercise together against cyber attacks. It is assumed that the more the number of exercises increases, the better mutual trust gets.

To conclude; first of all, 'NATO ought to use its dedicated Co-operative Cyber Defense Centre of Excellence in Tallinn to clarify the terminology, thus making it easier for allies to understand each other and co-operate' [28]. Secondly, the legal ambiguity of using ACD options before or during the cyber attacks should be compromised. Moreover, every single effort should be put to build mutual trust by doing combined cyber exercises. Last, but not the least; it is considered that

NATO has to adopt a comprehensive approach in order to take steps for the CIP.

V. Conclusion

Cyber threats are getting more dangerous each day. The more the world gets connected, the more our systems are vulnerable. Although security of every item in the connected world is important, some of them are vital. Those sectors can be named as telecommunication, finance, civil aviation, railways, electricity, gas, governmental/administrative services, medical services, water works, and logistics. Naturally, protecting these "critical infrastructures" has the utmost priority in case of a cyber attack.

In future, it is estimated that cyber attacks will be even more sophisticated and current cyber defense methods may not be adequate. Hence, active cyber defense options seem to be the effective solution to respond to an advanced cyber attack. Advanced cyber attacks tend to target the critical infrastructures of a state. Therefore, CIP by ACD stands as an important factor in terms of an effective cyber defense. However, ACD is not easy to implement, and it may cause some legal controversy.

As an important military organization, NATO is trying to develop its cyber defense capabilities. To achieve this, it has taken some important steps. However, it seems NATO may not be able to counteract to an advanced cyber attack effectively. To promote mutual cyber trust, NATO and other international organizations should exercise even more, clarify issues regarding the definition of critical infrastructure, solve the legal problems related to ACD, and have a comprehensive approach of CIP by ACD means.

References

[1] S. Lachow, Irving, "Active Cyber Defense A Framework For Policymakers", *Policy Brief*, pp. 1, February 2013.
[2] A Websense White Paper, "Advanced Persistent Threats and Other Advanced Attacks" rev. 2, pp. 1, 2012.
[3] Hutchins, Eric M, Clopperty, Michael J. Amin, Rohan M, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" pp. 2, November 21, 2010.
[4] A Websense White Paper, "Advanced Persistent Threats and Other Advanced Attacks" rev. 2, pp. 1, 2012.
[5] Kaspersky Lab, "Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide." Accessed November 19, 2013. http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide.
[6] Fryer-Biggs, Zachary, "Cyber security: merging and acquisitions", *Atlantic Organization for Security (AOS) Brief*, pp. 2, September 2011.
[7] Software Dell.com, "An Anatomy of a Cyber-Attack", Accessed November 1, 2013. http://software.dell.com/documents/anatomy-of-a-cyber-attack-ebook-24640.pdf.
[8] Wong, Tiong Pern. "Active Cyber Defense: Enhancing National Cyber Defense." Ph.D. dissertation, Naval Postgraduate School, Monterey, December 2011,
[9] S. Lachow, Irving, "Active Cyber Defense A Framework For Policymakers", *Policy Brief*, pp. 1, February 2013.
[10] Ünver, Mustafa, "Kritik Altyapıların Korunması", *Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı,* syf 6, Mayıs, 2010.
[11] "Action Plan on Information Security measures for Critical Infrastructure", *Decision by Information Security Council*, pp. 2, 13 December, 2005.
[12] US Government, "Homeland Security Act 2002", Accessed August 5, 2013. http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.
[13] Homeland Security Presidential Directive / HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection" Accessed August 9, 2013. http://www.fas.org/irp/offdocs/nspd/hspd-7.html.
[14] Communication from the Commission to the Council and the European Parliament, "Critical Infrastructure Protection in the Fight against Terrorism" pp. 2, October 2004.
[15] Ünver, Mustafa, "Kritik Altyapıların Korunması", *Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı,* syf 17, Mayıs, 2010.
[16] NATO Parliamentary Assembly, "162 CDS 07 E rev 1 - The Protection of Critical Infrastructures", Accessed August 18, 2013. http://www.nato-pa.int/default.asp?SHORTCUT=1165.
[17] "NATO Prague Summit Declaration" Accessed March 03, 2013. http://www.nato.int/docu/pr/2002/p02-127e.htm
[18] Çiftçi, Hasan. "Her Yönüyle Siber Savaş." TÜBİTAK Popüler Bilim Kitapları, pp. 52, Ankara, 2012.
[19] Cooperative Cyber Defense Centre of Excellence, "Cyber Defense", Accessed on 3 December 2013, https://www.ccdcoe.org/
[20] NATO Cooperative Cyber Defence Centre of Excellence, "Mission and Vision" Accessed July 18, 2013. https://www.ccdcoe.org/11.html.
[21] NATO Parliamentary Assembly, "173 DSCFC 09 E bis - NATO and Cyber Defence" Accessed August 18, 2013. http://www.nato-pa.int/default.asp?SHORTCUT=1782.
[22] Smedts, Bart. "NATO's Critical Infrastructure Protection and Cyber Defence." *Royal High Institute for Defence Center for Security and Defence Studies*, pp. 14, July 2010.
[23] NATO Communications and Information (NCI) Agency, "End to End Capability Delivery" Accessed September 18, 2013. http://www.ncsa.nato.int.
[24] The NCIRC Technical Centre, "The NCIRC Technical Centre's Mission", Accessed September 18, 2013. http://www.ncirc.nato.int/.
[25] Transatlantic Policy Briefs, "Coming to Terms with a New Treat: NATO and Cyber Security" pp. 3, January 2013.
[26] Ibid:4
[27] Çiftçi, Hasan. "Her Yönüyle Siber Savaş" TÜBİTAK Popüler Bilim Kitapları, pp. 52, Ankara, 2012.
[28] Transatlantic Policy Briefs, "Coming to Terms with a New Treat: NATO and Cyber Security" pp. 3, January 2013.

Serkan Yağlı, was born in Kırıkkale/TURKEY in 1981. He graduated from Turkish Military Academy in 2004. He served in Turkish Army as an artillery officer between 2004 and 2012. He received M.S. degree in "Total Quality Management" from Beykent University. He is currently studying at Turkish Army War College. He is interested in cyber warfare, cyber security, critical infrastructure protection and active cyber defense.