Journal of Naval Science and Engineering
2014, Vol.10, No.2, pp.1-24

CYBER DEFENSE IN DEPTH: DESIGNING CYBER SECURITY AGENCY ORGANIZATION FOR TURKEY

Dr.Kerim GOZTEPE[1] Recep KILIC[2] Dr.Alper KAYAALP[3]

[1-,3]*Army War College, Dept. of Operations&Intelligence, 34330, İstanbul, Turkey.*

[2]*War Colleges Command, Army War College, Yenilevent-34330, İstanbul, Turkey.*

kerimgoztepe@gmail.com, rkilic40@gmail.com, allperkayaalp99@gmail.com

Abstract

With the increase of mobile devices and the implementation of the concept of "internet of things", human beings began to live entirely in a cyber-world besides physical world. This unexpected expansion of cyberspace has caused a vulnerability to all kinds of cyber-attacks. Today, the number of attackers and correspondingly the number of attacks are increasing, but the attackers' knowledge levels are diminishing. This inverse ratio in cyber threats force organizations and states to take more comprehensive security measures. Developed countries have begun to accept cyber space as a fifth operational domain after land, sea, air and space. The study reveals that designing cyber security agency for Turkey is a crucial issue in terms of cyber defense in depth for an effective homeland cyber security. In this paper, we suggest eight layered "defense in depth architecture" that is proposed "cyber security agency organization" for Turkey. We believe this structure provide more effective real-time information sharing between governmental organizations also.

DERİNLİĞİNE SİBER GÜVENLİK: TÜRKİYE SİBER GÜVENLİK AJANSI ORGANİSAZYONU TASARIMI

Özetçe

Mobil cihazların artması ve "nesnelerin interneti" kavramının uygulanması ile, insanoğlu tamamen fiziksel dünyanın dışında bir siber-dünyada yaşamaya başladı. Siber uzayın bu beklenmedik genişlemesi, her türlü siber saldırı karşısında savunmasız kalmasına neden oldu. Bugün, siber saldırganların sayısı ve siber saldırı sayısının artmasına rağmen saldırganların bilgi düzeyleri azalmaktadır. Bu ters orantı, örgütleri ve devletleri, siber tehditlere karşı daha kapsamlı güvenlik önlemleri almaya zorlamaktadır. Gelişmiş ülkeler kara, deniz, hava ve uzaydan sonra siber uzayı beşinci operasyonel etki alanı olarak kabul etmeye başlamışlardır. Çalışma, Türkiye için siber güvenlik ajansı tasarımının, etkin bir ülke siber güvenliği açısından derinlemesine siber savunmanın önemli bir konu olduğunu ortaya koymaktadır. Bu makalede, tasarlanan Türkiye "siber güvenlik ajansı kurumu" için sekiz katmanlı" derinliğine savunma mimarisi" önerilmiştir. Biz bu yapının, devlet kurumları arasında daha etkili gerçek zamanlı bilgi paylaşımını sağlayacağına inanıyoruz

Keywords: Cyber securtiy, Cyber defense in depth, Designing cyber security agency organization, Turkey

Anahtar kelimeler: Siber güvenlik, Derinliğine siber savunma, Siber güvenlik ajansı organizasyonu tasarımı, Türkiye

1. INTRODUCTION

In early 1990s, with the prevalence of internet and other IT assets in the world, the concept of space disappeared in a sense and intercontinental communication became easier than pushing a button. Twenty years ago, cyberspace was an utopia, but it is now a reality itself [1]. This unexpected expansion of cyberspace has brought with itself vulnerability to all kinds of cyber-attacks [2]. These attacks can be performed by; countries, political

adversaries, terrorists, industrial spies, hacktivists, hackers, resentful and unconscious users.

Internet security annual reports state not only states are spying on each other in cyberspace, but also originating sophisticated cyber-attack techniques [3]. The concept of cyber war consider more attacks for penetrating networks. These can be motivated by political objectives instead of financial gain [4]. By the next decade network security is likely to be one of the biggest threats for security in the world. In this regard, a line and understanding need to be developed including crucial information systems and critical physical infrastructure, such as water and electricity services, airports, gas transmission and distribution facilities of all kinds [5].

Most states are aware of an inevitable cyber conflict in the coming years. Generaly, they have designed cyber warfare procedures [6]. Cyber security experts claim that cyber warfare takes place all around us with its intensity. During peace time, sides are detecting each other's vulnerabilities, traps, open doors, logic bombs, penetrating to the defense systems and even inserting the rear doors with microchips for entire systems. In this way, intermingling of war and peace is dragging on the world similar to the Cold War instability. Stuxnet like cyber weapons that target critical infrastructure will increase in the next period (Stuxnet involves sophisticated techniques using legal digital signatures) [7] .

This paper argues that it is not sufficient just to have a powerful army. The power of the computer and the information is strong enough to include states. This study makes recommendations to states considering cyber warfare and began to prepare deployment of fifth military force.

2. DEFENSE IN DEPTH

Cyber-attacks carried out on Estonia in 2007 constitute the turning point in terms of alarming the world to take into account the phenomenon of cyber threats [8].Beside, "Aurora" code-named attacks to Google and other sites in 2010; the "Conficker" called worms targeting Microsoft products in 2008;

Stuxnet worm aiming to harm a nuclear program, and many more new attack methods showed that they were as real as conventional threats [9]. The explosion of a pipeline by not using explosives but logic bombs constitutes the best example for impacts of cyber-attacks to the real world [10].

Today, it is estimated that many states have active operational cyber weapons development program. Cyber weapons are being developed secretly and there is too little information about them [11]. It is seen that all developed countries are sensitive and aware of the danger. Each country approach to the subject includes completely different methods and strategies. Turkey is left behind in terms of cyber institutionalizations and arrangements made for the issue.

Turkey is one of the first target countries exposed to cyber-attacks and has become directly or indirectly the base of these attacks. An integrated cyber defense model should be developed in order to increase the level of cyber-defense capability of the country that ensures the homeland security. Therefore, defense in depth approach must be carried out to configure cyber-defense activities that guarantee the security of the systems targeted by cyber threats.

The purpose of defense in depth approach is to maintain a system against any particular attack using several independent methods. National Security Agency (NSA) apply a comprehensive approach to information and electronic security. Defense in depth concept has emerged as a model to isolate key resources with protective layers [12]. Opinions about layered structure elements are varied though studies in the world. For example, NSA layers are called as people, technology and operations. According to another source, it is ranked as device, application, computer, network and physical [13],[14].

Different types of “defense in depth” approach is applied by most of states or organizations. It is a known fact that a simple cyber protection is not sufficient for a real protection according to literature [15],[16].

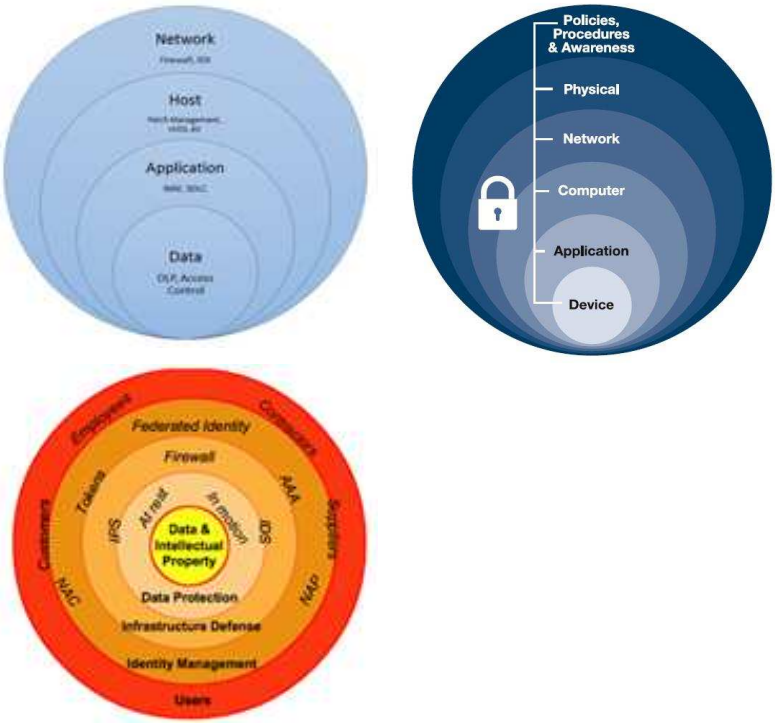

Figure 1: Different types of "defense in depth approaches [15],[16],[17]

"Defense in depth" uses multiple "layers" to protect an organization's critical assets [17]. This means if an attack manage to enter main system, an outer or inner layer will step in for protection (Figure 1). We believe that to establish defense in depth architecture does not provide a perfect security. However, it strengthens and complicates cyber security level. States or organizations need to develop more complex defense strategies to prevent composite attacks.

We proposed more comrehensive "defense in depth" architecture for Turkey in order to cope with complicated cyber attacks. The layers of defense in depth architecture which should be applied for Turkey is shown in Figure 2.

It depicts integrated model of a homeland cyber defense. The component of proposed model is given in Section 3.

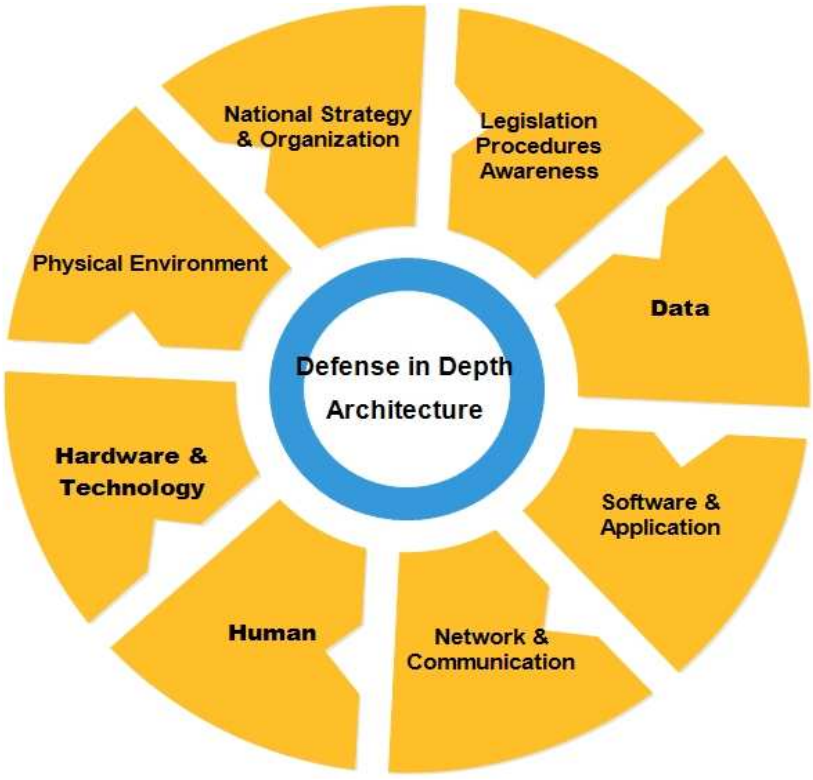

Figure 2. Layers of defense in depth architecture.

3. DEFENSE IN DEPTH AND COMPOSING CYBER SECURITY AGENCY FOR TURKEY

Defense in depth is concept of layered defense that is not a new term in the information technology arena [14],[15]. Nevertheless, new technologies develop rapidly, systems become more detailed and it is difficult to secure. Thereby, cyber experts must understand system behavior and plug vulnerable holes as soon as possible. Establishing cyber security agency for Turkey should provide more dynamic and comprehensive structure to avoid

cyber attacks. This study offers a new organizational structure for state cyber security.

3.1. National Strategy and Organization

Cyber security development for national policy and strategy needs success of measures taken against cyber-attacks [18]. Improving effective cyber security policies is a time consuming and generally cost too much. It also requires all departments involvement within an organization. Therefore, it is important to ensure full coordination of all the elements specified in the framework of national strategies and policies. The United States (US) main cyber security organization chart can be seen in Figure 3 in terms of a sample approach. US cyber security structure involves “National Protection and Programs Directorate” and “Office of Cybersecurity & Communications” departments under “US Department of Homeland Security”. “Office of Cybersecurity & Communications” department has nine sub-departments in this structure. There are three main department that is necessary because of US supremecy in this structure.

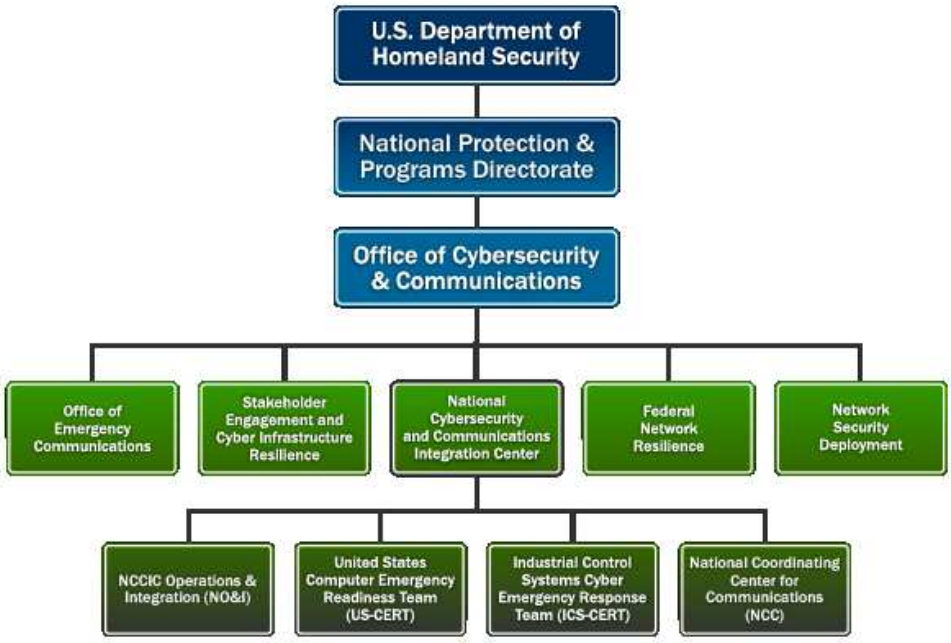

Figure 3. US National Cybersecurity and Communications Integration Center [19]

A good cyber security strategy can be implemented by determining the activities demonstrated in strategic, operational and tactical levels. Some vital issues for designing Turkey cyber security organization startegy is given below:

- It is required to take support of the parliament when creating comprehensive cyber defense strategy.
- Goverment should consider cyber issues with organizations, private sector and reassessment of existing laws/regulations.
- Cyber security strategy can be realized with the decision taken at the top level. For this purpose; cabinet and national security council should gather with cyber security agenda once a year.
- Cyber security agency should be set up to serve as an executive organ, undersecretary at the Ministry of Defense that will implement the decisions taken by the cyber security board.

- It would be the right approach connecting Armed Forces Cyber Defense Command to this agency and employment of Cyber Defense Commander to serve as Chief of Cyber Security Agency in terms of directing from one center.

Proposed "Cyber Security Agency" organization chart for Turkey is shown in Figure 4. Beside, organization chart explanation is written in the following text. APPENDIX A explains interaction between Cyber Security Agency structure and "defense in depth" architecture

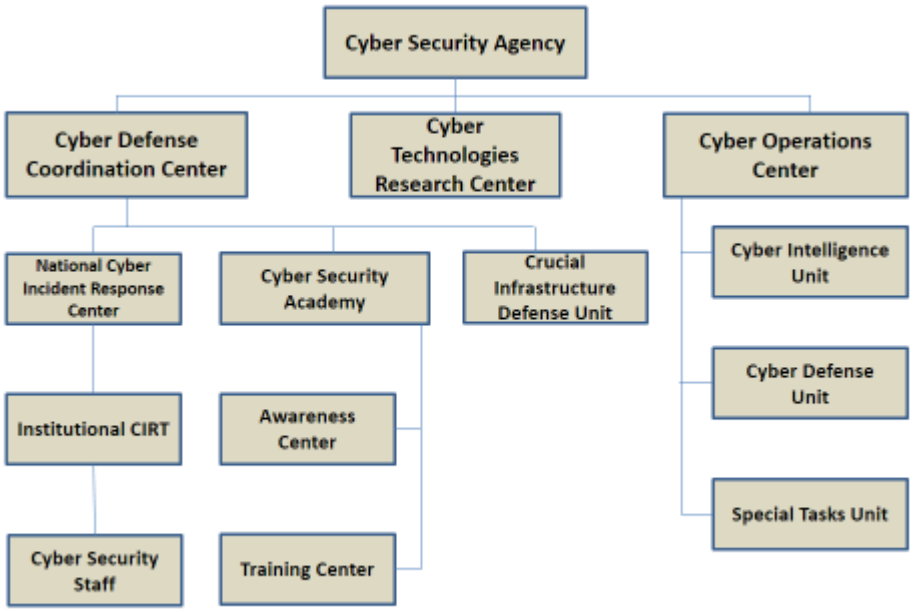

Figure 4. Proposed "Cyber Security Agency Organization" chart for Turkey

3.1.1. Cyber-Defense Coordination Center

In a politically motivated war, public service agencies and organizations have limited opportunities to withstand attacks. Specialized central public

institutions/organizations' support may improve the success rate. A well-designed Cyber Defense Coordinating Center should increase the success of counter attack and total defense capabilities. National Cyber Incident Response Center (NCIRC) and Institutional CIRT (Computer Incident Response Teams) should have units that serve 24/7 basis as the Cyber Reaction Force to perform predetermined procedures before the attack, during the attack and after the attack give chance to overcome Cyber Attacks with minimum causalty.

Cyber experts are designers and leaders of proposed cyber security agency organization study. Therefore, cyber security academy should be an institution where nationwide awareness activities will be carried out and a variety of courses should be given to cyber security staff. Besides cyber security instructions, guidelines and action plans should be prepared and come into effect by experts within this structure.

3.1.2. Cyber Technologies Research Center (CTRC)

All kinds of research on cyber technology should be made in this unit. Important cyber projects should be conducted at CTRC. These may be Malware Analysis, Advanced Persistent Threat (APT) analysis, national malicious software database, intrusion detection and prevention systems, data leakage prevention systems, monitoring experienced cyber incidents and software in the world in 24/7 basis serving, botnets infiltration, solving command and control systems [20].

3.1.3. Cyber Operations Center

Development of secret technologies is implemented and applied as counter cyber-defense in this unit. Under this center there will be Cyber Intelligence Unit which will perform the proactive defense measures; Cyber Attack Units carrying out small-scale operations; and long-term quality operations are being carried out. Recent studies showed that, laws, regulations or agreements are not obstacle for the development of offensive capabilities [21]. Therefore, armies have begun to search more reactive tactical cyber-defense to strengten strategic cyber-defense policy [22]. With these insights,

units can be formed in order to launch cyber-attacks against enemies' information systems in terms of tension or war.

Open source intelligence is another research area for proactive defense concept. New intelligence missions may vary in a wide range of activities such as national security, economy, space, cyber space, media operations and support foreign diplomacy [23]. For example Britain's domestic intelligence agency, MI5, informed UK businesses against to People's Liberation Army about cyber espionage [24]. Today it is a fact that information technology is changing the way of intelligence. Therefore, offensive and defensive cyber operations are key elements of information warfare. Cyber Operations Center experts may obtain large amount of data for national security over the net.

3.2. Legislation, Procedures, Awareness

It is not easy to make an international definition of cyber space. This causes an uncertainty on boundaries of the cyber space and international law on cyber-attacks. Maybe a common understandings on cyber conflict, and the responsibilities of states would help to create an international framework for a definition. Cyber-crimes research institutes and forensics departments should be established in universities in order to define rules of cyber space. Forensic computing and information technology issues should be taken into curricula in faculty of law and our information should be brought to the level of understanding, evaluating and interpreting the expert's report. New branches that require technical expertise in the field of data security, information and communication technologies should be as a technological necessity.

For this purpose, an independent forensic computing institution should be established in Turkey. Management of information assurance belonging to different system must be carried out within the framework of national standards. National information system standard should be prepared in accordance with this standart and all IT processes put into practice across the country. Public space should be provided in "corporate information

assurance management system" program. In most of security breaches, lack of awareness in user behavior is indicated as a basic factor. Turkey is one of the most exposed countries against cyber threats. It is very important to see awareness from individuals to state for our future. Creating cyber security culture and execution of a comprehensive national awareness program including government, educational institutions, private sector, civil society organizations and individuals is strongly important.

3.3. Physical Environments

It is not likely to provide precise security only with strong economy but the economy and physical security measures can be accepted as a piece of overall national security puzzle [25]. Internet Service Providers (ISP) have a unique and special role in country's cyber fore front [26]. The authority and obligation should be given to ISPs to prevent information security breaches. ISP should be held responsible for violations of their subscribers and it should be taken under provisions in their contracts with their subscribers.

Internet Exchange Point (IXP) is a physical infrastructure that Internet Service Providers can transfer data among themselves without a transit carrier. Thanks to these infrastructures countries can keep their content within their so they diminish attacks rooted from abroad. Because Estonia did not own any IXPs which are usually located in developed countries at the date it was attacked, traffic carried out over international internet exchange points and suffered due to cyber-attacks. Today, establishment of IXP in metropolises, have great importance in terms of cyber defense. Therefore, locating IXP centers in different Turkish cities becomes curucial for cyber security agency organization. Big data transfers over big IXPs in the west countries can cause information privacy weakness against both that countries and those fiber route passing.It is also important to keep input and output data at certain points.

Cyber defense coordination centre is important for keeping the source and destination basis filters ready against attacks and creation of effective external defensive line. Each environment, in which valuable information is produced, transmitted and stored, is critical. Physical security issues like

zone and building safety, gate security, biometric recognition systems, TEMPEST security, backup and disaster recovery measures should be applied in a very strict way as indispensable elements of cyber security [28]. TEMPEST is a collection of protection standarts from spying. It is also about leaking electromagnetic emanations, beside encompasses sounds or mechanical vibrations.

3.4. Human

It is called "The chain is only as strong as its weakest link". The most important element and at the same time the weakest link in the chain of information assurance is human being. It is obvious that the more human factor is informed the more it will be safe. System security level can keep up as much as people's awareness level. Staff security and reliability working at all levels of cyber defense architecture emerge as a separate issue, as well. It is the fact that most physical or electronic attacks can be assisted by an insider.

Being dominant on future technologies primarily requires educated manpower. It includes Research&Development (R&D) personnel in the fields of science and technology, scientist and engineers and field work technical staff. In terms of our national interests, this potential should be directed to the needs of our country.

To solve the problem, it is not sufficient to approach cyber security topic from a technical perspective only. In order to achieve radical perspectives and obtain foresight some studies including managerial approaches like strategic chaos management, fuzzy logical decision support systems, investigating psychological causes of cyber-crime and its impact on society should be done. Academics should be directed to the examination of cyber security in terms of basic disciplines.

3.5. Hardware and Technology

In today's world, it is known that developed countries are carrying out high cost R&D activities on new weapon technologies in order to obtain an

advantage in the battlefield. In terms of a possible crisis, you may not be able to provide defense technologies and equipment ordered from a second country for national security; but with a strong economy and scientific investments you can be self-contained. At this point it is important that in many developed countries IT sector including software and hardware products, declared as "strategic industry".

It is not possible to determine or know whether cyber security technologies supplied from abroad contains back door or malware such as Trojan horses. Therefore, following of next generated, innovative and intelligent technologies, national and the original development and the provision of government support has big importance [29]. R&D based supply should compose the main axis of the public procurement policy which considers the strategic priorities in the field of technology. In the realm of defense system supply we should not be act according to the principle of free competition but to the principle of national security. Hardware and Technology issue should be handled with Turkish Hi-Tech scientific firms for a better cyber security agency organization.

3.6. Networking and Communications

Isolation of critical infrastructures and the creation of the national network that provide data exchange with other government institutions should be completely separated from the internet [30]. Layered national networks on different levels of confidentiality should be established depending on the nature of the information processed and the implementation of different security policies. Indeed, national judicial network and Ministry of Defense attacks have confirmed the fact that these networks are necessary. The US is the pioneer country with its GovNET Project [31]. However, an intranet is not safe as they are supposed to be. In particular, when the number of users increase and the corporation grows security decreases. Systems that feel safe against outside world are in fact unprotected for insider attacks. It is estimated that 40% rate of attacks emerge from the local area networks [32]. In this case, next to the taking precautions against attacks from outside, local area network security emerges as another crucial issue. Thus, proposed

cyber security agency organization in this study includes both local and international networks.

3.7. Software and Applications

Software and application issue is another main theme for cyber security agency organization. Software/application maintenance&update can be provided across the country by a central service. Cyber experts should ensure that all the software used in public institutions and systems are in the same standards as much as possible. To prevent application-level attacks is difficult because of user identity [33]. At this point, the traditional approach to ensure security, on physical layer, network and system, should be completed with software security.

We should be aware of the fact that security is an issue that cannot be added to software product afterwards [34]. Some states have developed their national operating systems for more secure cyber environment. Hence, open source national operating system should be used primarily in national institutions and state-owned enterprises (SOE) which produce technologies. It will also be an appropriate solution to get rid of sleeping Botnets [35]. It is evaluated that implementation of incentives programs necessary for local production of cyber warfare self-defense elements like firewall, intrusion detection system and etc. This is an important issue for projects like "national tank" or "national fighter". For this purpose threat analysis laboratories should be established for the development of national integrated cyber security software. Worldwide cyber events should be followed by a center and national malware database should be established and shared for academic uses.

3.8. Data

Country information assets, country weaknesses, health information, critical economic data, military information and critical information are intended to be protected and they are subject to cyber defense [36]. Even though security measures fail in any way, a certain level of protection should be

provided by encryption algorithms, by digital signatures and steganography based measures in all, production, and transportation and storage stages of data [37].

Proposed “defense in depth architecture” eight layers and activities associated with each layer should be carried out at national level. But it is not limited to these measures. Such measures like firewalls, antivirus software, intrusion detection/prevention systems, honeypot, burglar alarm, network monitoring and management software, logging and backup should be carried out by the system administrators and security professionals in the appropriate layer.

4. CONCLUSION

In recent years, economic, technologic and political changes, global terrorist events have changed definition of threat and war. Cyber experts name this new era as information age. Political circumstances and terror events have changed perception of states from "classic threat" to "asymmetric". Definition of battlefield is not the same before. Distinction between war and peace has blurred.

By the next decade cyber world is likely to be one of the biggest threats for security in the world. Cyber warfare may occur among information systems of conflicting groups and countries. Developed countries are aware of cyber threats and have already launched cyber warfare. Cyber warfare takes place all around us with its intensity. In this regard, a cyber-defense line and understanding need to be developed including those involving crucial information systems and critical physical infrastructure.

The most important step for achieving powerful cyber defense is to put forth a strategy and a suitable cyber-defense structure. In this study, it is revealed that an eight layered defense in depth architecture can be considered as an appropriate model for Turkey. Besides, cyber security agency organization design with its components is offered in this paper. The framework presented in this paper views cyber defense strategy not as a defense

architecture, but rather as a multi-dimensional organization by three main center: cyber defense coordination center, cyber technologies research center, and cyber operation center. We should be aware that without field called combat cyber war, a state can not ensure its' security

References

[1] Cavelty, M. D. (2007). Cyber-security and threat politics: US efforts to secure the information age. Routledge.

[2] Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. Communications Surveys & Tutorials, IEEE, 14(4), 998-1010.

[3] Kumar, G., & Kumar, K. (2014). Network security–an updated perspective.Systems Science & Control Engineering: An Open Access Journal, 2(1), 325-334.

[4] Dipert, R. R. (2014). The Future Impact of a Long Period of Limited Cyberwarfare on the Ethics of Warfare. In The Ethics of Information Warfare (pp. 25-37). Springer International Publishing.

[5] Knapp, E. D., & Langill, J. T. (2014). Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Syngress.

[6] Colarik, A., & Janczewski, L. (2012). Establishing cyber warfare doctrine. Journal of Strategic Security, 5(1), 31-48.

[7] Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40.

[8] Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?. Journal of Conflict and Security Law, 17(2), 212-227.

[9] Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365-404.

[10] Rid, T. (2012). Cyber war will not take place. Journal of Strategic Studies, 35(1), 5-32.

[11] Wagner, P. J., & Wudi, J. M. (2004, March). Designing and implementing a cyberwar laboratory exercise for a computer security course. In ACM SIGCSE Bulletin (Vol. 36, No. 1, pp. 402-406). ACM.

[12] Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing, 25(2), 357-370.

[13] Chi, S. D., Park, J. S., Jung, K. C., & Lee, J. S. (2001, January). Network security modeling and cyber attack simulation methodology. In Information Security and Privacy (pp. 320-333). Springer Berlin Heidelberg.

[14] Wu, F. J., Kao, Y. F., & Tseng, Y. C. (2011). From wireless sensor networks towards cyber physical systems. Pervasive and Mobile Computing, 7(4), 397-413.

[15] Steve Ocepek, (2014), Unraveling the Onion: A New Take on Defense-in-Depth, http://blog.securestate.com/kill-chain/ , Access time, March 2015.

[16] Proactive Protection Through Industrial Networks, http:// www. industryweek.com/ rockwell-automation-connected-industrial-enterprise/proactive-protection-through-industrial-networks , Access time, March 2015

[17] Rod Starrett, (2006) How to protect data in an IP world , http://www.eetimes.com/ document.asp?doc_id=1274286, Access time, March 2015.

[18] Chabinsky, S. R. (2010). Cybersecurity strategy: A primer for policy makers and those on the front line. J. Nat'l Sec. L. & Pol'y, 4, 27.

[19] National Cybersecurity and Communications Integration Center, https://www.us-cert.gov/nccic.

[20] Amoroso, E. (2012). Cyber attacks: protecting national infrastructure. Elsevier.

[21] Lin, H. S. (2010). Offensive cyber operations and the use of force. J. Nat'l Sec. L. & Pol'y, 4, 63.

[22] Geers, K. (2010). The challenge of cyber attack deterrence. Computer Law & Security Review, 26(3), 298-303.

[23] Steele, R. D. (2002). The new craft of intelligence. OSS International Press.

[24] Pearson, I. L. (2011). Smart grid cyber security for Europe. Energy Policy, 39(9), 5211-5218.

[25] Rajkumar, R. R., Lee, I., Sha, L., & Stankovic, J. (2010, June). Cyber-physical systems: the next computing revolution. In Proceedings of the 47th Design Automation Conference (pp. 731-736). ACM.

[26] Lori, M. (2009). Data security in the world of cloud computing. Co-published by the IEEE Computer And reliability Societies, 61-64.

[27] Xu, K., Duan, Z., Zhang, Z. L., & Chandrashekar, J. (2004, January). On properties of internet exchange points and their impact on as topology and relationship. In Networking 2004 (pp. 284-295). Springer Berlin Heidelberg.

[28] Goztepe, K. (2012). Designing Fuzzy Rule Based Expert System for Cyber Security. International Journal of Information Security Science, 1(1), 13-19.

[29] Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731.

[30] Goztepe, K. (2014). Recommendations on Future Operational Environments' Command Control and Cyber Security, 7th International Conference on Information Security and Cryptology, 55-58.

[31] Pan, X., Slettengren, J., Nkurunziza, I., Munyarugerero, H., & Karera, N. I. GovNET project Final Report, KTH MSc project in Communication Systems Design, Stockholm, October 2006.

[32] Akritidis, P., Chin, W. Y., Vinh The Lam, Sidiroglou, S., & Anagnostakis, K. G. (2007, August). Proximity Breeds Danger: Emerging Threats in Metro-area Wireless Networks. In USENIX Security.

[33] McGraw, G. (2006). Software security: building security in (Vol. 1). Addison-Wesley Professional.

[34] Sisaneci, I., Akin, O., Karaman, M., and Saglam, M. "A Novel Concept For Cybersecurity: Institutional Cybersecurity", 6th International Conference on Information Security and Cryptology, Turkey, Ankara, Sep. 20-21, 2013, pp. 89.

[35] Stone-Gross, B., Cova, M., Gilbert, B., Kemmerer, R., Kruegel, C., & Vigna, G. (2011). Analysis of a botnet takeover. Security & Privacy, IEEE, 9(1), 64-72.

[36] Caliskan, M., Ozsiginan M., and Kugu, E., "Using Virtualization Technologies for Intrusion Detection and Prevention Systems Security", 7th International Conference on Application of Information and Communication Technologies (AICT), pp. 1-5, 2013.

[37] Mouratidis, H., & Giorgini, P. (2007). Integrating security and software engineering: an introduction. Information Security and Ethics: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications, 200.

APPENDIX A

Definition of Proposed "Cyber Security Agency Organization" Departments and Interaction between "Layers of Defense in Depth Architecture

		Interaction Between "Layers of Defense in Depth Architecture" and "Cyber Security Agency Departments" **"+" shows interaction degree. More "+" means interaction is strong.**							
Cyber Security Agency Organization" Departments	**Definition of Proposed "Cyber Security Agency Organization" Departments**	**National Strategy And Organization**	**Legislation, Procedures, Awareness**	**Physical Environment**	**Human**	**Hardware And Technology**	**Network, Communication**	**Software and Application**	**Data**
Cyber Security Agency	**Name of proposed cyber agency for Turkey**	+++	+++	+	+	+	++	+	+
Cyber Defense Coordination Center	**Department that coordinates cyber incidents with governmental organizations**	++	++	++	+++	++	++	++	++

National Cyber Incident Response Center	**Response center to unexpected and sudden cyber-attacks.**	+	+	++	+++	+++	+++	+++	+++
Cyber Security Academy	**Educational center for cyber experts**	+++	+	+	+++	++	++	+++	+++
Crucial Infrastructure Defense Unit	**Cyber team that secure vital infrastructures of Turkey**	+	+	+++	+++	+++	+++	+++	+++
Institutional CIRT	**Computer Incident Response Team members are cyber experts who educates new experts in the institute.**	+	++	+++	+++	+++	++	+++	+++
Awareness	**Informs cyber experts of governments about**	+++	+++	+	+++	+	+	+	+

Center	**latest cyber events/sophisticated attacks/cyber problems**								
Cyber Security Staff	**People who educated on cyber related science. Cyber experts**	+	+	+++	+++	+++	+++	+++	+++
Training Center	**Cyber security education center.**	++	+++	+	+++	+	+	+	+
Cyber Technologies Research Center	**Research/Development center for cyber technologies.**	+++	+++	+++	+++	++	++	++	++
Cyber Operations Center	**Main center that coordinates cyber operations.**	++	++	+++	+++	+++	+++	+++	+++
Cyber Intelligence Unit	**Cyber experts who gather intelligence over the Net.**	+	+	+	+++	+++	+++	+++	+++

Cyber Defense Unit	**Cyber team that plan cyber operations.**	+	+	+++	+++	+++	+++	+++	+++
Special Tasks Unit	**Cyber experts who use high technology to fulfill special cyber operations**	+	+	+++	+++	+++	+++	+++	+++