Institutional Cybersecurity from Military Perspective

Muhammer Karaman*‡, Hayrettin Çatalkaya*, Celil Aybar*

* War Colleges Command, Army War College, Yenilevent-34330, İstanbul, Turkey. Tel: +90 212 398-0100

‡Corresponding Author; Tel: +90 212 398-0100, e-mail: muammerkaraman29@gmail.com

Abstract- In the time we are living in, the nonlinear increase, usage and reliability on information communication technologies (ICT) are going to move forward. In this digital environment, people, institutions and government take necessary precautions ranging from personal to strategic level and adapt themselves to live or operate in that new form of environment. When we consider a country' cybersecurity efforts as a whole, it starts with individuals at the bottom, institutions, firms and military organizations at middle and government at the top. Ensuring a robust cybersecurity policy in a country, requires all levels (individual, institution, government) to be at the same standard. While the government level cybersecurity strategy documents generally present a comprehensive approach, the institutional level cybersecurity roadmaps, action plans are generally not present or overlooked. Being one of the main elements of a country, military organizations should be prepared to operate in this new form of operational environment that is full of malwares, advanced persistent threats (APT) and cyber espionage software. In this study, institutional cybersecurity from the military perspective is analysed in the light of possible challenges, organizational structure, the military decision making process (MDMP) and cybersecurity workforce.

Keywords- Institutional Cybersecurity, military organizations, MDMP, cyber operations, cybersecurity workforce.

1. Introduction

Due to living in an interconnected world with smart devices and appliances in cyberspace, the cyber security issue has always taken the significant role and emerged as a planning factor almost in every public or private institution. Having a close relation with information security, the cybersecurity term has evolved the former as a result of the increasing number of highly cost security breaches, irreversible prestige loss. Along with the use of internet, the use of cutting edge technologies in private and military organizations, ranging from tactical to strategic level like command, control and satellite systems, has put the cybersecurity issue much more forward and entailed cybersecurity to be a more comprehensive concept over traditional information security. The concept of information security procedures has proved insufficient due to the complex nature multidimensional and strategic effects of cyber attacks, advanced persistent threats (APT) [1].

In today's security environment, most of the efforts are being done to reach the data running on systems, structured data, and the data that is not digitalized yet, unstructured data. Although not handled in this study, one of the main efforts in this context is to make the unstructured data digitalized, the structured data [2]. Whatever be the commercial, military and intelligence purpose, multiple ways to access all kinds of data, information and knowledge require that the confidentiality, integrity and availability of information are ensured. The cyber intelligence and espionage efforts are getting more and more complex sometimes igniting hard debates and conflicts between nations. How the institutions, military organizations will manage to operate in this new form of environment will be handled in this study. In section two, we discuss institutional

cybersecurity and challenges will be discussed. In section three, we discuss how institutional cybersecurity becomes an integral part of cyber operations and military decision making process (MDMP). In section four, the cybersecurity workforce and military organizational structure will be discussed and finally proposals for more effective structures will be presented for a better cybersecurity approaches from military perspective.

2. Institutional Cybersecurity

Cybersecurity efforts generally start from the government or strategic level and continue to the bottom, individual level with different methods, tools and goals. In this frame, the institutional cybersecurity, taking its place between government and individual level, constitute the main body of the cybersecurity efforts. Government level cybersecurity activities generally are issuing a national cybersecurity strategy document, establishing a national cybersecurity center or national computer incidents response teams (CIRT) and nation wide coordination of cyber incidents. The institutional cybersecurity activities [3] are first of all to obey and ensure the necessary standards coming from the upper level and to form an institutional roadmap that clearly address all possible cyber incidents and also the processes during cyber incidents and all the other activities boosting up the cyber efforts. Finally, the individual level cyber activities start with situational awareness on cyber incidents, personal cybersecurity measures, obeying the procedures, rules and not overlooking cyber issues. Considering the roles and responsibilities of jobs at all three levels, our assumption is that the institutions that are most vulnerable are those that form the government and have critical infrastructures. The difficulty in envisioning the cyber threats in current times and the enlargement of cyberspace encompassing a new operational environment for military organizations, there are naturally significant challenges that need to be addressed to avert failures. National Cybersecurity Framework Manual by NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) has articulated important national dilemmas that should be addressed as shown in Table 1 [4].

Table 1. Main dilemmas of national cybersecurity [1] [4]

1	Stimulate the Economy vs. Improve National Security
2	Infrastructure Modernization vs. Critical Infrastructure Protection
3	Private Sector vs. Public Sector
4	Data Protection vs. Information Sharing
5	Freedom of Expression vs. Political Stability

Similar dilemmas and challenges are present more or less for institutions as well. One of the main dilemmas that institutions may face is Security vs. Privacy. The cyber attacks are happening all around the world every second. While these attacks can range from a simple code breaking to an industrial hacking and stealing from companies intellectual property assets, plans, designs and drafts etc., worth billions of dollars. The institutions may therefore wish to watch every click of their employees. In that case, the privacy of employees can be violated and overlooked. There are also some other dilemmas for institutions as well, that are shown in Table 2 [1].

Table 2. Main dilemmas of institutional cybersecurity

1	Institutional Cybersecurity vs. Privacy
2	Privacy vs. Information sharing [5]
3	Homegrown human resource vs. Outsourcing [6]
4	Open source vs. Licensed software [7]
5	IT Security Cost vs. Institutional Cybersecurity
6	Technical vs. Administrative.
7	Cooperation vs. Loss of Reputation [8]

The institutional dilemmas stated above are generic and therefore they may increase or decrease according to the type, mission, center of gravity and area of focus of institutions. The effect of social media and intelligence particularly open source intelligence (OSINT) that is cheap and easy to implement, are the key factors to be reckoned with in public and military institutions [9]. The increasing use of smart devices and the widespread use of social networks like Facebook, twitter,

LinkedIn, Instagram and so on has forced the institutions to implement not only technical but also administrative precautionary measures. Especially when it comes to enforcing and sustaining the procedures, strategic awareness and leadership play a crucial role. Besides these challenges, the resiliency of command and control structure and crisis response plans in case of cyber incidents is vital for getting away with less harm.

Script kiddies, state sponsored or freelance hackers use OSINT due to its ease to access the data, information or even knowledge [10]. Actually there is limited amount of knowledge that can be found on internet, but there is a huge amount of data that hackers can simply gather and transform into information and knowledge thanks to the free tools that are accessible on the internet. Consequently the knowledge management processes of terrorists and enemy hackers enable them to attain critical information either by metadata analysis of open source data available on public websites or with the use of social networks [11].

After gathering user and system information, through various sources, and with internet of things (IoT), attackers can transform the information to form emulated versions of the organizational structure of an institution and track the personnel on social networks with masked accounts to serve their future objectives like phishing and cyber espionage attacks [12].

Uploading documents, photos and announcements to institutional websites can be seen a mundane activity within an institution if you underestimate the possible cyber risks. The prevailing use of social networks and metadata obtained from uploaded contents can reveal a quiet amount of data and information to adversaries.

While well known companies gather data from their users to provide better solutions and maximize their income, it can be wrong to assume that the terrorist organizations and the enemies do not or can't deal with the big data. The data attained from a single source can easily be cross checked with other services thanks to IoT, like social networks, online profiles or any thing taking its place in internet. Even the photos of an activity in an institution can yield about many details of the event (place, time, the make of device and so on) with their exchangeable image format (EXIF).

A metadata analysis of collected photos from various sources, can be performed using free tools available on internet. After that kind of effort, a great deal of valuable information can be attained, like relations of people and their friends, where and when they had met, which route they track etc. Seemingly unimportant and trivial things may be some invaluable information for terrorists. Taking into account these kind of challenges coming with internet and social networks, a comprehensive cyber approach should be applied balancing the security and privacy with clear and concrete procedures in institutions. In this context and in terms of our perspective, the main and growing challenges of institutional cybersecurity are as shown in Table 3 below:

Table 3. Main and growing challenges of institutional cybersecurity

1	Lack of institutional cybersecurity strategy and roadmap.
2	Cyber manpower and workforce.
3	Strategic Cyber Awareness and Leadership. (Top-Down)
4	Open Source Intelligence, metadata efforts.
5	Big Data Analytics.
6	Bring your own device (BYOD).
7	Increasing use of social networks.
8	Cyber Crisis Response Planning
9	Resilient Command and Control.
10	Interoperability of systems and subsystems among other institutions.

3. Cyberspace Operations (CO) and Military Decision Making Process (MDMP)

According to Joint Publication 3-12, Cyberspace Operations (CO), there are several cyberspace capabilities whose main purpose is to attain the objectives in or through cyberspace [13]. The commanders, whether in battlefield or in headquarters should be aware of the cyber use, its advantages and risks, in military operations. Today's and tomorrow's security environment could not be thought apart from information communication technologies (ICT) which is

supposed to ensure confidentiality, integrity and availability of information when and where it is needed [14]. In order to succeed in cyberspace and attain the cyber superiority, armies should effectively implement cyberspace operations. In some military organizations, cyber capabilities are managed together or under the frame of electronic warfare units [15].

For instance, the leading countries in the world handle cyber and electronic in a same context and merge these two activities like cyber electronic warfare activities (CEWA) [16] due to the close relations of these two areas in military operations. When we analyze the cyberspace operation, it is divided in three parts; offensive cyberspace operations, defensive cyberspace operations and DOD information network operations [16].

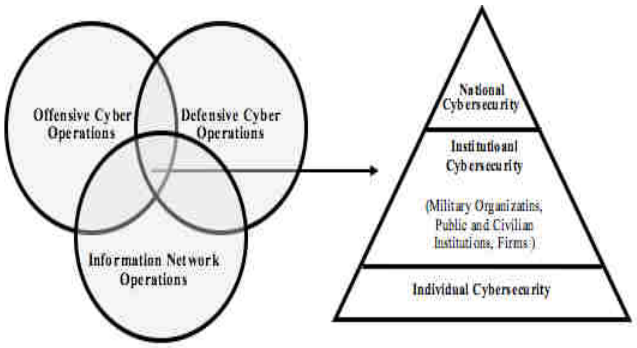

Fig. 1. Three Interdependent Functions [FM 3-38] interaction with cybersecurity hierarchy model.

In the operation's process, planning is handled with art and first understanding and then visualizing a fact and putting forward the ways to reach the target [17]. Operational planning can be divided in two areas, conceptual and detailed planning [17], [18], [19]. The conceptual planning deals with a more comprehensive, creative and critical thinking approach in order to put the operational environment in a framework applying an appropriate operational design. The detailed planning is the execution of military decision making process (MDMP) after getting the commander's initial planning guidance [20].

MDMP is a continuous and recurrent system that facilitates the leaders to understand the situation, analyse the mission and develop course of actions [20]. Planning cyberspace operations whether within electronic warfare concept or stand alone, requires detailed planning leading to specific MDMP. Cyberspace or cybersecurity is a functional area of battlefield supporting operations, regardless of an operation ongoing, alone, or as a sole tool or solution achieving military objectives. We argue that, in future, the integration of conventional operations and cyberspace operations becomes a *sine-qua-non* for military success.

By following the steps of MDMP [21], starting from the defining and accepting the mission and preliminary examination of it, CO should be analysed through all the steps and finally put forward just like other battlefield functional areas detailing how it can support the operations. When an operational design is prepared by a group of staff before planning, or simultaneously, operational cyber effects should also be considered under the name of "*Cyber Operational Design*." The need for operational design from cyber perspective stems from the complex nature and strategic effects of cyber threats. Therefore, before or along with the MDMP, cyber operational design should be prepared in order to support commander's decision and help the MDMP to be aligned in terms of cyber. An awareness of the strategic effects of enemy's information systems and critical infrastructures, CO can be the commander's main method to operate in the battlefield before deploying any of its units.

3. Cybersecurity Workforce, Manpower and Organizational Structure

In order to provide talented and qualified cyber manpower for military organizations there should be a cybersecurity workforce strategy section within an institutional cybersecurity roadmap. Considering the sources of manpower, the eligible workforce should be secured at the very beginning from military high schools, from military academies and civilian cybersecurity dedicated personnel. However, it is not easy to work with talented hackers in a military organization, the flexible working hours and other facilities should be provided in that environment. It must be also ensured that a clear definition of roles, job descriptions and duties should be communicated in order to classify the areas of responsibilities and to abide by the rule of law.

The distribution of responsibilities of cyber workforce can be information assurance, cyber intelligence, operations (offensive and defensive), and maintenance in general. As a result of cyberspace operational planning in MDMP, intelligence requirements are going to help identify the adversary's efforts, activities and even center of gravity. Therefore, cyber intelligence gathering from multiple sources with multiple tools will have an important role in cyberspace operations planning [22]. However, to find and recruit the talented, dedicated hackers, programmers and systems administrators to work for your institutions is not an easy job. But if institutions demonstrate that they have a high level of cyber situational awareness and a special interest in cyber security and also promise a good salary, it may attract those people to apply to your institutions. In this context, cybersecurity recruitment exercises such as "*capture the flag*," are of great importance in order to attract and identify potential and skilled cyber patriots [23].

One more important factor in attracting talented cybersecurity workforce in military institutions is coming together with universities and having a close collaboration and coordination in cyber events like conferences, cyber camps, workshops and cybersecurity exercises across nation-wide. These kinds of events are going to boost cyber situational awareness and bring together the talented people and provide a social environment where people can share their know-how and tacit and explicit knowledge. Whether these kinds of events can be organized by public institutions or private ones, military high school or academy students should be encouraged to participate in those activities personally or with designated teams. For instance, in U.S military academy, WestPoint, and some other institutions like National Security Agency (NSA) and Department of Homeland Security (DHS) are organizing such cyber events [24]. In order to form a robust and effective cybersecurity workforce for military organizations those initial steps should be be taken into account as follows:

- Having a cyber workforce planning section in the institutional cybersecurity roadmap or document,
- Job descriptions for cyberspace activities should be clearly specified and documented, no ambiguous areas should be left,
- Civilian contractors meeting the required military standards, having the necessary international certificates in their fields, should be recruited and assigned in cyberspace operations' positions.
- Talented civilian contractors should especially be used on job and master-apprentice trainings,
- Resilient cyber workforce planning should be envisaged and necessary adjustments for service time of contractors should be implemented carefully.

Many countries have established their cybersecurity organizations both in government level and institutional (military) level. From military perspective, when we think of an operation, we also think of several main elements like intelligence and logistics. Particularly the intelligence activities precede the operation in order to provide all the necessary information and knowledge, putting forth the action, about the enemy then a suitable reaction can be given to a situation. In this context, in the MDMP process supporting the commander's decision and operations order, intelligence becomes one of the core elements of operational plan.

Therefore, in military cyber organizations there should be a close interaction and interoperability between cyber and intelligence units. The same issue is also valid for electronic support (ES) activities that support all three main elements: (Electronic Attack (EA), Electronic Protection (EP) and Electronic Support (ES)) of electronic warfare (EW). Electronic support activities require close collaboration with intelligence measures since they focus on searching for radiated electromagnetic energy for threat analysis [25].

In Fig.2, a proposed cyber command and its relation to intelligence command is shown. Due to the strategic nature of cybersecurity, the cyber command should be able to respond to the needs of the army rapidly and with little or no bureaucratic inertia. Therefore, it should be as proximate as possible to the commander of the army. Here, cyber and electronic units can be separate or integrated as a single command too. The costs and benefits of single command of cyber and electronic

units can be analysed in terms of operability, efficiency, effectiveness, bureaucracy and cost.

It should be remembered that before arranging the organizational structure of the cybersecurity units, following action items should be prepared, executed and sustained:

- Clearly stated national and institutional cybersecurity strategy document [26] or a roadmap,

- Government or military level cybersecurity end states,

- Legal frame of cyberspace operations and electronic warfare activities

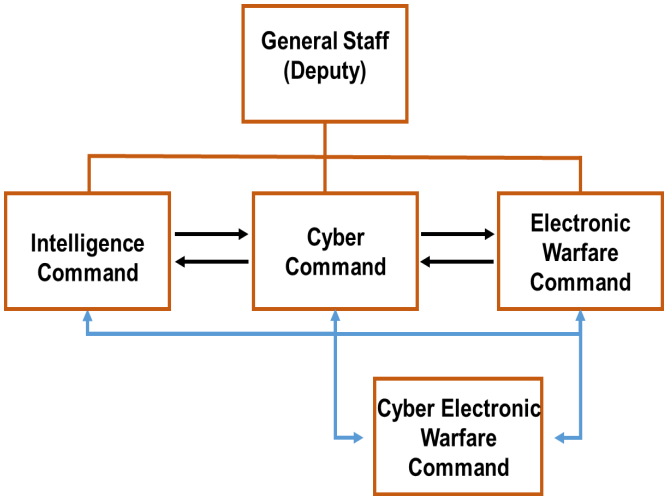

Fig. 2. The proposed organization of cyber command in military organizations that has close relation with electronic warfare and intelligence units.

3. Conclusion

The understanding and handling of the cyberspace, cybersecurity efforts vary from country to country. Some countries see the picture more comprehensively [4] including national critical infrastructures, electromagnetic spectrum, electronic warfare and cyber intelligence activities in the big picture. Therefore, those countries see the cyberspace and cyber activities as a strategic means or a new domain within the operations environment [27]. On the other hand, some other countries perceive cyberspace as equal to internet and therefore, they simply see the cybersecurity as equal to information security.

The complex and destabilizing cyber attacks, whether a denial of service attack, a cyber espionage or an advanced persistent threat (APT), have shown that the level of risk is high and no one is immune to being a subject of cyber threats. In public or civil organizations, the institutional cybersecurity can be achieved by having and sustaining a comprehensive approach like envisioning challenges, dilemmas, cyber risks especially emanating from social networks, preparing an institutional cybersecurity roadmap or action plan, updating information security procedures to compose cyber issues, balancing between privacy and security in institutions.

However, from a military perspective the things that civilian institutions should do forms the tier one in military organizations. In addition to these, tier one, military organizations should be prepared to operate in cyberspace whether cyber is a supportive of a full operation (conventional, urban warfare, peace support etc.) or an operation on its own. Regarding the destructive effects, collateral damage and killings of both civilians and military personnel, cyber wars can play an important role in preventing the killings and casualties in battlefield.

In such a chaotic era, the military organizations need to prepare for the worst by establishing resilient and cyber command structure, interoperable and synchronized planning efforts with electronic warfare command. Due to the changing character of wars from conventional to unconventional, symmetric to asymmetric and hybrid wars, cyber operations need to be designed to defense and sustain the military assets.

Acknowledgements

This study is an extended version of the same article presented in May 2015 at The International Science and Technology Conference at Harvard Medical School, USA, that is designed by International Journal of Arts and Science (IJAS).

References

[1] I. Sisaneci, O. Akin, M. Karaman, and M. Saglam. “A Novel Concept for Cybersecurity: Institutional

Cybersecurity", 6th International Conference on Information Security and Cryptology, Turkey, Ankara, Sep. 20-21, 2013, pp. 89.

[2] H. Cintiriz, M. N. Buhur and E. Sensoy. "Military Implications of Big Data", International Conference on Military Security Studies, ICMSS-2015, Turkey, İstanbul, War Colleges Command, March 10-11, 2015.

[3] J. Ferwerda, N. Choucri and S. Madnick. "Institutional Foundations for Cyber Security: Current Responses and New Challenges"

[4] A. Klimburg, Ed., National Cyber Security Framework Manual. NATO CCD COE Publications, 2012.

[5] B. Adelmann, "Cispa is Big Brother's Friend," 2012.

[6] S. Alexander, "Rise of Outsourcing Poses New Cybersecurity Problems," 2011.

[7] B. Gourley, "Open Source Software and Cyber Defense," 2009.

[8] "Security Task Force: Public-Private Information Sharing," 2012.

[9] L. Ablon, M.C. Libicki and A.A. Golay, Markets for Cybercrime Tools and Stolen Data,

[10] Open Source Intelligence: A Strategic Enabler of National Security, CSS Analyses in Security Policy, Vol.3, No.32, April 2008.

[11] M. Karaman, H.Catalkaya. "Institutional Cybersecurity: "A Case Study of Open Source Intelligence and Social Networks", International Conference on Military Security Studies, Turkey, Istanbul, March 10-11, 2015.

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

[13] Cyberspace Operations, Joint Publication (JP) 3-12 (R), 2013.

[14] J. Spagnuolo-Loretta, R. Brockway and J.C. Burget. "Risk-Based Assessment and Scoping of IV&V Work Related to Information Assurance", September 14, 2014.

[15] Cybersecurity and Cyber Warfare Preliminary Assessment of National Doctrine and Organization, Center for Strategic and International Studies (CSIS), 2011.

[16] Cyber Electromagnetic Activities, FM 3-38, Department of The Army, Available: https://armypubs.us.army.mil/doctrine/index.html.

[17] The Operations Process, FM 5-0, Department of The Army, March 2010.

[18] S.C. Feng and Y. Zhang. "Conceptual Process Planning-A Definition and Functional Decomposition".

[19] A.E Kober. "Bridging the Planning Gap: Linking Conceptual Army Design to Military Decision-Making". School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas, 2010.

[20] Military Decision Making Process FM 101-5, Department of The Army.

[21] Battle Staff Guide. Army National Guard Battle Command Training Center Leavenworth Fort Leavenworth, Kansas 66027-2346, August 2010.

[22] I. Kilaz, A. Onder, and M. Yanik. "Manpower Planning and Management in Cyber Defense." 13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece, 2014.

[23] O. Akın, et al. "Siber Durum Farkındalıgını Artırmada Etkili Bir Yontem: Bayragı Yakala (Capture the Flag)", 6th International Conference on Information Security and Cryptology, Turkey, Ankara, Sep. 20-21, 2013.

[24] Homeland Security Grant Program. Supplemental Resource: Cyber Security Guidance, U.S. Department of Homeland Security, Fiscal year 2014.

[25] N. Yasar, F.M. Yasar, and Y. Topcu. "Operational Advantages of Using Cyber Electronic Warfare (CEW) in the Battlefield." SPIE Defense, Security, and Sensing. International Society for Optics and Photonics, 2012.

[26] K. Goztepe. Cyber Defense in Depth: Designing Cyber Security Agency Organization for Turkey. Journal of Naval Science and Engineering 2014, Vol.10, No.1, pp.1-24.

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