A Novel Concept for Cybersecurity: Institutional Cybersecurity

İbrahim Şişaneci, Osman Akın, Muhammer Karaman, Mehmet Sağlam

Abstract—Broader use of digital technologies in all aspects of our lives, exponential expansion of cyberspace, along with complex and advanced cyber threats, lead us to reevaluate the cybersecurity concept that has been involved in our documents and directives differently or inadequately. One of the main issues in this evolving cyberspace is the perception of cybersecurity. Encapsulating a large scale of elements from individual to government level, cybersecurity approach particularly has two outstanding dimensions; national and institutional cybersecurity. Complicating, shape shifting and stretching the imagination, emerging cyber threats have demonstrated that traditional security needs and approaches do not fulfill cybersecurity requirements and can no longer withstand robustly to emerging cyber threats. In this study, a novel concept, "Institutional Cybersecurity", is suggested instead of information security (InfoSec) processes being used in present state by institutions.

***Index Terms*—Institutional Cybersecurity, Cyber risk, Dilemmas and Challenges of Cybersecurity, Evolution of Cybersecurity**

I. Introduction

Information technology has become widespread in our life that contains from cell phones and computers to more complex systems such as Information Technology (IT) infrastructures, power grids, air traffic management systems, industrial manufacturing, and banking sectors. It seems they will continue to be in upward trend in the future. Security of these IT components will be more important due to the increase of cyber attacks day by day. The more the critical infrastructures depend on the information system, the more cyber risks we have to expect.

Previous cyber attacks have showed that existing vulnerabilities in networks and information systems host serious damage risks [1]. In recent years, in addition to traditional cyber attacks, new attack techniques such as Advanced Persistent Threat (APT) related attacks, using zero-days, rootkit malwares and etc., have been used in many incidents that have a specific target to be attacked. Therefore, cyber attacks need to be handled comprehensively due to lack of attribution and geographical boundaries, low costs, low risk for the attacker, and a large scale of applicability. Hence, technical measures are not enough alone to cope with these kinds of complex cyber threats.

I.Şişaneci is with the Comp.Eng.Dept., Gebze Institute of Technology, Gebze-Kocaeli,Turkey, (e-mail: sisaneci@gyte.edu.tr).
O.Akın is with the Comp.Eng.Dept., Hacettepe University, Ankara,Turkey, (e-mail: oakin@hacettepe.edu.tr).
M.Karaman is a Cyber Security Expert, (e-mail: muammerkaraman29@gmail.com).
M.Sağlam is with the Comp.Science Dept., VirginiaTech, Virginia, USA, (e-mail: msaglam@vt.edu)

The terms as InfoSec, Information and Communication Technology (ICT) security, cybersecurity, etc. have utilized to define different concepts to address a wide variety of risks. In traditional cybersecurity perception, familiar terms are frequently used such as ICT security, InfoSec, information assurance, cybersecurity and so forth. By the dramatic up growth in the complexity of malwares and computer viruses, institutions could be vulnerable to cyber attacks due to the emerging cyber risks. Therefore, from now on emerging cyber risks should be elaborately redeemed and scrutinized in a new sense of cybersecurity awareness (c-saw). However, advanced multi-dimensional and complex cyber attacks necessitate and implicitly bring forth some other definitions and concepts like National Cybersecurity, Individual and Corporation-level InfoSec, and so on.

In this study, the evolution of cybersecurity is reviewed and the need of a new cybersecurity concept is emphasized. Besides, a new concept to provide institution-level cybersecurity is also proposed. The term "institution" is used for public/private companies that have infrastructures under potential cyber risks and critical services. This new concept enables us to understand cyber risks better than traditional approaches and basically contains cybersecurity challenges, components and main principles in institutional-level.

The organization of this study is as follows. In Section 2, we briefly define crucial terms as InfoSec, cyberspace and cyber threats. In Section 3, we briefly review InfoSec approach and evolution of cybersecurity, giving special emphasis on its challenges and dilemmas. Next, in Section 4, we propose a concept, "Institutional Cybersecurity", in particular the main features and principles of Institutional Cybersecurity, and components of institutional cybersecurity. Finally, the conclusions and future work are presented in Section 5.

II. Cyber Environment & Security Terms

A. Cyber Environment

Cyberspace: The cyberspace defined as "the notional environment in which communication over computer networks occurs." or "A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" is growing rapidly [2].

Cyber Risk: Cyber risk, inherently exists in all IT assets, is a kind of risk which occurs in a variety that from individuals to international organizations that have critical IT assets. Cyber risk is specified as a group of risks, which differs in technology, attack vectors, means, etc., rather than one specific risk. The value of cyber risk is equal to

multiplication of probability and impact of cyber threats. Moreover, Cyber risks have two characteristics as having great potential impact and low probability (Fig. 1) [3]. Although traditional security focuses on many threats having high probability and average level impact on IT assets, cyber risk based security deals with cyber threats having low probability and very high impact on IT assets.

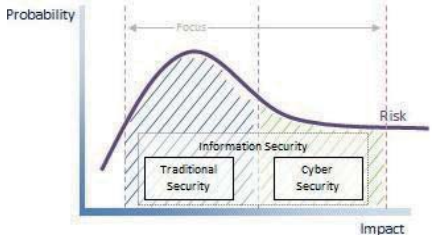

Fig. 1. Probability and Impact of Cyber Risk [3]

Cyber threats and attacks: After specifying the cyber risk, there is another crucial term, cyber threat. Cyber threat can be defined as a potential situation that covers the distortion of information, changing the information by unauthorized people, disclosing or stealing information or interrupting its accessibility. The source of cyber threat may be a single computer that is infected, or that may be a bot-net which could consist millions of computers. Therefore, even a single computer in the cyber environment, both with the information it contains and its connection the other systems, can be a source for hackers to reach critical systems. A list of cyber attack trends is presented (in Table I) conducted between 1990s and 2013. Briefly, cyber attacks can be vary from a dummy computer virus (Morris Worm) to an Advance Persistent Threat (APT), and they are evolving continuously and exponentially. These cyber attacks could be classified as: Cyber Crime, Hacktivisim, Cyber Terrorism, Cyber Espionage and Cyber Warfare [4].

B. Security Terms

The question "How can an IT asset get secured in this dangerous and complex cyberspace?" is origin of many security terms. The terms InfoSec, information assurance (IA), and computer security (CompuSec) are key cyber related security terms.

Information Security

Currently, the terms InfoSec and IA are frequently used. InfoSec is defined as protecting the information or information system from unauthorized access, modification or destruction in NIST Glossary of Key Information Security Terms [5]. According to the international standard ISO/IEC 27002:2005, Information Security is "preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved".

Information Assurance

A more comprehensive term than InfoSec is information assurance that includes practice of InfoSec. IA is "the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. IA includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data. It uses physical, technical and administrative controls to accomplish these tasks. While focused predominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form" [6].

TABLE I
CYBER ATTACK TRENDS

-Internet social engineering attacks	-Windows-based remote access trojans (Back Orifice)
-Network sniffers &Packet spoofing	-Email propagation of malicious code
-Analysis of vulnerabilities in compiled software without source code	-Wide-scale trojan distribution
-Cyber-threats & bullying (not illegal in all jurisdictions)	-Targeting of specific users
-Automated probes and scans	-Anti-forensic techniques
-GUI intrusion tools	-Wide-scale use of worms
-Automated widespread attacks	-Sophisticated botnet command and control attacks
-Widespread, distributed denial-of-service attacks	-Mobile device(phone) Android exploiting
-Industrial espionage	-Advance Persistent Threat (APT) [61]
-Executable code attacks (against browsers)	-Cloud Attacks
-Session-hijacking	-Embeded malwares
-Widespread attacks on DNS infrastructure & using NNTP to distribute attack	-Hardware based malicious components
-"Stealth" and other advanced scanning techniques	-Old school malwares for spying (MiniDuke)

Cybersecurity

As we come to cybersecurity term, there are many definitions in use, however we would present a couple of these: First, cybersecurity is "the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this" [2] Second, "Cybersecurity is the sum of efforts invested in addressing cyber risk, much of which was, until recently, considered so improbable that it hardly required our attention" [3]. Third, from International Telecommunication Union's (ITU) point, it is "The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment."

Institutional Cybersecurity

As a result of rapid changes in cyber environments, expansion of cloud computing, and residual use of mobile devices particularly in institutions, cybersecurity related terms should be re-handled with a broader line of sight. Therefore, in terms of institutional cybersecurity, a novel concept need has emerged. We suggested a new concept, Institutional Cybersecurity, to symbolize and fit for all institution-level cybersecurity issues. The Institutional Cybersecurity is the capability which consists of InfoSec components and cooperation with other cybersecurity partners and cybersecurity awareness from the cyber risk perspective.

III. INFORMATION SECURITY APPROACH AND EVOLUTION OF CYBERSECURITY

A. General Security Concept & Technological Developments

Security concept contains components that are assets, risks, threat, vulnerabilities and countermeasures. Generally,

security is a process of the selection and implementation of security controls (also called countermeasures) which help to reduce the risk posed via vulnerabilities [7]. The security process of information and elements that are related to information is evolving as the technology behind it. The motivations of this evolution are mainly changing assets and risks that have pose by the increase of dependency on Internet, the set of assets is growing every day as mentioned above. Unfortunately, variety of cyber risks is growing faster. Because of the highly interconnected nature of these assets, every vulnerability has impacts on the others that makes the evolution exponential. On the other hand, the change in security side is inherently behind this technological evolution. The new assets that are connected to the network and their vulnerabilities must be analyzed, or even in some cases they may get attacked by competitors to be understood what the real consequences could be. Then the solutions would be developed to address these emerged risks. However, conceptualization, developing strategies, and doctrines follow that.

B. Information Security Approach

Understanding Information Security approach and the evolution of cybersecurity requires analyzing the question that how/why the key concepts have emerged? The concepts that must be taken into account in this case are ICT security, InfoSec, and cybersecurity.

ICT security is the intersection area of InfoSec and cybersecurity. ICT security covers information technology infrastructure such as computers, computer networks, data centers as its assets. Furthermore, these assets could be extended in InfoSec to all sorts of information to be secured. By this definition, InfoSec covers not only the data in ICT but also the information which is not stored or transmitted via ICT (Fig.2). Nevertheless, as stated above, cybersecurity conceptually covers both information and non-information based assets that have posed risks via ICT. The types of these assets include a wide variety of what that also covers critical national infrastructures, household appliances, and even also human.

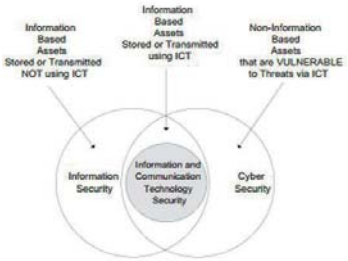

Fig. 2. Area of interest for Information and Cybersecurity [7]

As a matter of fact, in cyberspace, the assets need to take consideration could be anyone or anything that is accessible via cyberspace. Briefly, InfoSec intends to secure whole IT infrastructures and processes. But, due to its enormous size, that may not possible to secure cyberspace as a whole. Instead of this, cybersecurity focuses on eliminating vulnerabilities on IT assets.

C. Evolution of Cybersecurity

The concept of cybersecurity first appeared with cyber breaches. And then, it has taken the name of cybersecurity when cyber breaches damaged government networks. By the expansion of cyberspace, the concept of InfoSec becomes inadequate to address multi-dimensional and complex cyber attacks. For instance, one of the advanced cyber espionage malware, "Red October" targeted diplomatic and government institutions worldwide for at least five years which has been detected in January 2013 [8]. Another example is the Industrial Control Systems Computer Emergency Response Team (ICSCERT) report of the US Department of Homeland Security [9] has shown that; In the first half of the fiscal year 2013, (October 1, 2012–May 2013), the highest percentage of incidents reported to ICS-CERT occurred in the energy sector at 53%. For another example, as stated by Verizon 2013 security report [10], which reported 2012 alone consists of 47000 security incidents, show that the growth of recent data breaches alarm that the organizations to take new actions. These examples support the legitimacy of the new concepts such as National Cybersecurity, Individual and Corporational Information Security, Cyber Awareness (c-saw) and so forth. That is the current result of the ongoing evolution. The continuous national/international level InfoSec efforts or recommendation publications may not adequately address the risks of cyberspace. As the current situation, InfoSec efforts were limited to their InfoSec management systems which are developed in line with international standards such as ISO 27001, NIST-800 series and COBIT. The current versions of these international standards have failed to meet completely cybersecurity requirements. Many countries and international organizations have developed their cybersecurity strategies that mainly focus governance, cooperation and active defense. However, in institutional level, there is no international standard or guideline which consists cooperation, integration to national security and active defense to cope with cyber threats, such as APTs.

D. Challenges and Dilemmas of Cybersecurity

Due to the complex nature of cybersecurity, many challenges and dilemmas have been emerged from both national and institutional perspectives. For instance, in National cybersecurity Framework Manual, prepared by NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE), dilemmas that nations face and have to deal with as establishing, maintaining and enforcing cybersecurity are stated that are stimulate the economy vs. improve national security, infrastructure modernization vs. infrastructure protection, private vs. public sector, data protection vs. information sharing, andfreedom of expression vs. political stability [11]. Similar to national level challenges, institutions also need to cope with some dilemmas that may be filtered from national challenges or may be localized version of national ones. The outstanding dilemmas of institutional cybersecurity are IT security cost vs. institutional cybersecurity, privacy vs. information sharing, homegrown human resource vs. outsourcing, open source vs. licensed software, and cooperation vs. loss of reputation [12]-[13]- [14]-[15].

Due to widely diverse cyber attacks, mentioned in Table I, sustainable cybersecurity is no longer a solely responsibility of cybersecurity personnel. But, it is a common

responsibility of all personnel, stakeholders and partners. For instance, an employee, without having enough cybersecurity knowledge and awareness or who underestimates cybersecurity regulations taken by the institution, may anytime cause deadly losses. Thus, this incident may result sometimes loss of reputation, economic assets, and so forth [1]. Along with national and institutional dilemmas, institutional cybersecurity challenges must be analyzed to understand the constraints. These challenges could be listed as; lack of broader perception of cybersecurity, information sharing, legal issues (legal suspense), leadership, cost, human resource, expansion of cyberspace, infrastructure insufficiency, standards addressing the majority, building common cybersecurity picture, lack of metrics of cybersecurity, lack of coordination and information sharing, security and usability issues, bureaucracy, insider threats, migration plan (unprotected systems to secure systems), technological backward compatibility and etc, [16].

E. Lack of broader perception of cybersecurity

The challenges of cybersecurity can be diversified endemically to nations and institutions according to their line of sight to cybersecurity. For example, according to Dmitriy Ayrapetov, Director, Product Management, Dell SonicWALL; the major cybersecurity challenges for businesses through 2013 will come from: increase in exploit kits, increase in mobile device security threats and increase in sophistication of threats [17]. But it may vary across analyses of experts on cybersecurity field; from our perspective, the number one cybersecurity challenge for both national and institutional level is lack of broader perception of cybersecurity. And to bring sectors and institutions to a level of security standard depends heavily on national perception of cybersecurity issues that also makes that the challenge number one. For instance, some governments may choose to centralize the majority of decision-making mechanisms, while others may devolve this to a lower level according to a particular need (e.g., to build resilience and responsiveness into highly decentralized and mostly privately-owned critical infrastructure) [11]-[18]. This decision would mainly effects the body of national cybersecurity issue. The cybersecurity burden on private sector may not desired but, even the government side of cybersecurity is tightened, it is just as easy for a terrorist organizations or other state-sponsored actors to take out a private-sector entity that will really impact the nation [19].

IV. AN EMERGING CONCEPT: INSTITUTIONAL CYBERSECURITY

With emerging new cyber risks and more complex malwares, countries and international organizations like NATO, ENISA, etc. have been looking for new ways to fight against challenging issues [16]-[20]. The essential step for countries is to form a national cybersecurity strategy. Generally, in that kind of strategies; the importance of policies, cybersecurity countermeasures and some action plans are taken into account at upper levels. Even though these strategies and policies cover intensively military, intelligence and critical infrastructures, the institution-level cybersecurity is ignored. In order to provide a robust national level cybersecurity, we believe that institution-level cybersecurity should be initial step to take forward. When we look at the whole cybersecurity organization structure (Fig. 3), institution-level cybersecurity forms the body part of cybersecurity organization which contains the entities as individuals, public/private institutions, military, government, and international organizations. Since the body part has a critical role to interact with all other entities, it affects the success of upper level cybersecurity.

While the weakest link in InfoSec is human being, in terms of national security the weakest link is the weakest institution having critical infrastructures or cyber risks. Unlike stated in national cybersecurity strategies, in terms of institutional cybersecurity, not only institutions which manages critical infrastructure but also other companies having cyber risk should be taken into account to ensure a robust cybersecurity. For example, a software company, without having any critical infrastructure, could be a target for cyber attacks due to stolen software code or root driver (SIEMENS & Stuxnet case)[21].

Current trends (Table I) including a complex attacks such as Stuxnet case make the need of a new concept inevitable. To address this need, our proposed concept, Institutional Cybersecurity could be defined as; A comprehensive concept for ensuring robust and resilient institution-level cybersecurity by; providing cyber situational awareness, addressing emerging cyber risks, encourage inter and intra institutional cooperation and coordination, and presenting a flexible framework for its applicability, for public/private institutions having critical infrastructures or having cyber risks for their business continuity.

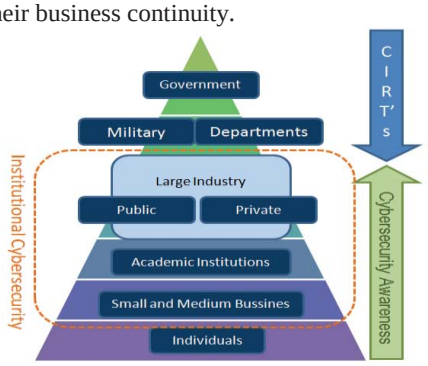

Fig. 3. Cybersecurity Organization Structure

Components and Principles of Institutional Cybersecurity

Our proposed concept provides a generic manner that every institution can adapt it for its own security needs to develop their institutional cybersecurity capability. To reach this goal, the main principles of Institutional Cybersecurity are presented as follows:

1-Cybersecurity approach must be holistic,

2-A flexible management style should be adopted,

3-Risk management-centered continuous improvement methods should be implemented,

4-In addition to coordination of public, private, academic, and non-governmental organization, international cooperation and information sharing should be bottom lines for security,

5- Transparency, accountability, ethical values, freedom of speech must be endorsed,

6-Setting balance between security and applicability is important.

In the light of these principles, in order to have efficient institutional cybersecurity, Institutional Cybersecurity should have fundamental components as presented (Fig. 4).

Policy, Strategy and Standards: Detailed cybersecurity policy, strategy and secure system management principles can help institutions to take the first step.

Cyber Risk Management: Cyber risks can be minimized and managed by utilizing efficient risk management mechanism to unveil all threats and vulnerabilities.

Vulnerability and Threat Management: According to advances in cyberspace, vulnerability and threat management could be handled under the cyber risk management. Vulnerability management should be supported by periodical vulnerability analysis/tests and penetration tests.

Central Incident Management: Efficient prevention, fast response and mitigation against to cyber attacks can be obtained by central incident management. And, active cooperation and collaboration to national cybersecurity can be achieved via the ability to central incident management including Institutional CIRT's.

Cybersecurity Awareness and Education: Human being is the weakest link in the security chain. Therefore, cybersecurity awareness and education programs must focus mainly human factor.

Log Management and Correlation: Possible attacks and data leakage could be detected in advance and preventive actions can be performed by utilizing efficient log management and correlation.

Secure Architecture: All institutional information technology infrastructures and architectures including business partners should be reviewed and questioned from the perspective of cybersecurity.

Legal Issues: The legal regulations always stand as the most important factor to enforce and ensure cybersecurity. To prevent privacy violation and to set liability processes, proper legal regulations must be set. Otherwise, countermeasures for providing cybersecurity such as monitoring personal information may pose risks for institutions.

Business Continuity: Business continuity plans must be harmonized with Institutional cybersecurity strategies and plans.

Technical Tools: Similar to ICT security, proper software and hardware including firewalls, IPDS, anti-virus software, etc. must be used to provide comprehensive cybersecurity.

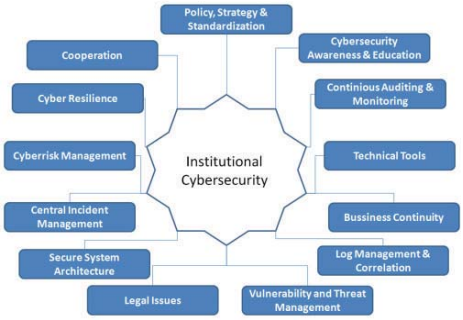

Fig. 4. Institutional Cybersecurity Components

Continuous Auditing and Monitoring: Auditing is a continuous process that contains audit tests or review procedures. Errors, policy violations, fraud, and misconducts should be audited in a timely manner to fill the control gaps and deficiencies. Monitoring is a mechanism that could be utilized to automate manual controls and processes or regular and frequent insights to avoid potential regulatory noncompliance, cyber attacks and malicious activities.

Cooperation: Cooperation with other cybersecurity partners and CIRT's are vital for institutions in order to set early warning mechanisms and effective resource sharing. Also, due to confronting asymmetric and organized cyber threats, government coordination with institutions and particularly with private sectors is inevitable.

Cyber Resilience: All efforts in the institutional cybersecurity management should be flexible enough to adapt to the dynamic developments in cyberspace. Cyber resilience can be defined in literature as "The ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities conditions, stresses, or attacks on the supporting cyber resources it needs to function." [22]. A Resilient Enterprise is able to withstand systematic discontinuities and adapt to new risk environments [23] or dynamically reinvent business models and strategies as circumstances change [24]. According to [22] a Resilience framework is able to include anticipate, withstand, recover and evolve steps.

Reaching the goal of using all of these institutional securitycomponents efficiently requires achieving cybersecurity objectives in institutional level. Furthermore, main goal of Institutional cybersecurity is to cooperate these components into an integrated framework in a resilient perspective. While securing the whole system, availability and usability could be ignored unintentionally. In order to avoid this situation, resilient management model should be performed. In this perspective, our proposed institutional cybersecurity concept contains resilient solutions for challenges. Another point is to manage all these components as an integrated framework requires a leadership. Through the principles and components of proposed concept above, challenges and dilemmas for institutional cybersecurity can be resolved considerably.

V. Conclusion and Future Works

All institutions, regardless of being public or private, should definitely expect and envision emerging cyber threats. With the help of revitalized InfoSec processes to fit a holistic cybersecurity concept and high level cybersecurity awareness, assessing and analyzing the potential and possible effects of complex and advanced threats will get less hard.

As a result of this research, it can be expressed that unless cybersecurity for institutions are handled in a broader perception, professional manner and presented as an integrated solution, it will have a higher possibility to be exposured and damaged by a cyber attack at any moment.

To date, many companies and institutions have had only IT departments. However, now, institutions having cyber risks should set up a cybersecurity or CIRTs. Hereby, the

institutional cybersecurity could be taken up in a more generic manner and encapsulates above-mentioned issues.

With the establishment of an institutional cybersecurity organization; the exploitable points in the system can be corrected by performing vulnerability test, the abnormality can be detected in real-time by monitoring logs, the situational awareness can be improved by applying scenarios, the risk assessment can be carried out by establishing integrated systems and probably the cyber attacks can be prevented before they start.

Due to their field-based and structural differences, each institution can prepare and follow a different cybersecurity road map peculiar to itself. But, as a first step, the recommended concept can be evaluated as an inception guide for institutions willing to start building a new cybersecurity capability.

In this study, we handled the cybersecurity issue from a new perspective for institutions and discussed in details. This new cybersecurity concept has also contributed and filled the conceptual absence of lower-governmental levels in cybersecurity organization structure.

Institutional cybersecurity will be an emerging fertile research area. There are many ways to extend this work in the future. For instance, we are planning to propose a new road map for institutions which is going to contain a transforming guideline to set forward a new concept in cybersecurity management processes.

REFERENCES

[1] H. Senturk, Z. Çil, and Ş.Sağıroğlu, "Cyber security analysis of turkey", International Journal of Information Security Science, vol. 1, no. 4, pp.112–125, 2012.

[2] Oxford dictionaries. (2013, Jun.) [Online] Available: http://oxforddictionaries.com

[3] M. Barzilay. (2013, May) "A simple definition of cybersecurity", [Online]Available:http://www.isaca.org/KnowledgeCenter/Blog/Lists/Posts/Post.aspx?ID=296

[4] M. Clancy, "Arm yourself for cyber war-Are you next?" *in Sibos Conference Panel 2012*, 2012.

[5] R. Kissel, "Glossary of key information security terms". *DIANE Publishing*, 2011.

[6] N. Seddigh, P. Pieda, A. Matrawy, B. Nandy, I. Lambadaris, and A. Hatfield, "Current trends and advances in information assurance metrics." in *PST*, 2004, pp. 197–205.

[7] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, 2013.

[8] KasperskyLabratuaries. (2013, Jun.), "Red october an advanced cyber espionage campaign targeting diplomatic and government institutions worldwide", [Online] Available: http://www.kaspersky.com/about/news/virus/2013/

[9] ICS-CERT. (2013, Jun.) "Ics-cert monitor report between april-june 2013 of department of homeland security".[Online]. Available: http://icscert.uscert.gov/sites/default/files/ICx-CERT Monitor AprilJune2013 3.pdf

[10] (2013, Jun.) Verizon. [Online]. Available: http://www.verizon.com

[11] A. Klimburg, Ed., "National cyber security framework manual". *NATO CCD COE Publications*, 2012.

[12] B. Adelmann, "Cispa is big brother's friend," 2012.

[13] S. Alexander, "Rise of outsourcing poses new cybersecurity problems," 2011.

[14] B. Gourley, "Open source software and cyber defense," 2009.

[15] "Security task force: Public-private information sharing," 2012.

[16] NATO. (2013, Jun.) Nato web site. [Online]. Available: http://www.nato.int, June,2013

[17] Techrepublic. (2013, May) "Cybersecurity challenges in 2013". [Online].Available:http://www.techrepublic.com/blog/security/cybersecuritychallenges in-2013/9038

[18] B. Karabacak and S. OZKAN, "Critical infrastructure protection status and action items of turkey," 2009.

[19] APCOForum.com. (2013, Jun.) "The cyber security challenge: The risk of inaction". [Online]. Available: www.apcoforum.com

[20] ENISA. (2013, May) "European network and information security agency glossary". [Online]. Available: www.enisa.europa.eu/act/res/files/glossary

[21] A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, "Stuxnet under the microscope," ESET LLC (September 2010), 2010.

[22] R. A. Caralli, J. H. Allen, and D. W. White, CERT "Resilience Management Model (CERT-RMM): A Maturity Model for Managing Operational Resilience". *Addison-Wesley Professional*, 2010.

[23] R. Starr, J. Newfrock, and M. Delurey, "Enterprise resilience: managing risk in the networked economy," *Strategy and Business*, pp. 70–79, 2003.

[24] L. Valikangas and G. Hamel, "The quest for resilience," 2009.

İbrahim Şişaneci is currently a PhD candidate in Comp.Eng.Dept., Gebze Institute of Technology (GIT). He received M.S. degree in Comp.Eng.Dept., GIT and BS degree in Comp.Eng.Dept. from Marmara University. His research interest are HCI, usability, InfoSec, Cybersecurity, data mining.

Osman Akın is currently a PhD student in Comp.Eng.Dept.,Hacettepe University. His research interest are cybersecurity, web based software, web based software security and computer vision.

Muhammer Karaman received his BS degree in Turkish Army Academy in 2005. His research interests are cyber war, cyber electronic war, cybersecurity.

Mehmet Sağlam received BS degree in Industrial Engineering from Turkish Naval Academy in 2009. He is currently a M.S. degree student in Department of Comp.Science, VirginiaTech. His research interests are Critical Infrastructure Protection and Cyber Warfare. In particular, his current research focuses on Power Grid Cyber Security.