Cyber Security Roadmap From Institutional Perspective

Muhammer KARAMAN, İbrahim ŞİŞANECİ

***Abstract*—Nowadays, cyber world has become indispensable through digital technologies are used extensively in all aspects of our lives . Besides many advanteges/facilities coming with the cyber world, mankinds is facing new threads.In this cyberworld, in addition to the classic security needs, every member which is from corporations to individuals needs cyber security. A novel concept Ïnsttitiaonal Cyber Securityïs suggested.This article shed light on cyber security institutions to ensure that there is a roadmap. In this article, a roadmap which will shed light on institutions to ensure cyber security is recommended . This roadmap against cyber threats contains cyber security elements such as policies, plans, awareness actities and works including technical and administrative measures.**

***Index Terms*—Cyber Security,Information Security,**

I. Introduction

NOWADAYS....XXXX. In this work, the word "institution" is used for public or private sector companies/corparations and state institution which have critical infrastractures.

Information technology has become pervasive in every way—from our phones and other small devices to our enterprise networks to the infrastructure that runs our economy. Improvements to the security of this information technology are essential for our future. As the critical infrastructures of the United States have become more and more dependent on public and private networks, the potential for widespread national impact resulting from disruption or failure of these networks has also increased.

Cyberattacks are increasing in frequency and impact. Adversaries seeking to disrupt the nation's critical infrastructures are driven by different motives and view cyberspace as a possible means to have much greater impact, such as causing harm to people or widespread economic damage. Although to date no cyberattack has had a significant impact on our nation's critical infrastructures, previous attacks have demonstrated that extensive vulnerabilities exist in information systems and networks, with the potential for serious damage. The effects of a successful attack might include serious economic consequences through impacts on major economic and industrial sectors, threats to infrastructure elements such as electric power, and disruptions that impede the response and communication capabilities of first responders in crisis situations.

This cybersecurity R and D roadmap is an attempt to begin to define a national R&D agenda that is required to enable us to get ahead of our adversaries and produce the technologies that will protect our information systems and networks into the future. The research, development, test, evaluation, and other life cycle considerations required are far reaching—from technologies that secure individuals and their information to technologies that will ensure that our critical infrastructures are much more resilient. These investments must tackle the vulnerabilities of today and envision those of the future.

dip not XXXX
dip not XXXX
dip not XXXX

II. Cyberspace And Cyber Threats

* The term of security should be re-defined in terms of cyber security with including the components of cyber space and emerging cyber threats. What is more important than bridging a new term between security and cyber security, is the perception and understanding of the individuals of institutions about the new aspects of security definition or redefined security term.

Definition of cyberspace "the notional environment in which communication over computer networks occurs." [2]

III. Cyber Security Approach

A. Current Concepts

Siber savunma, Siber Harekat vd.Bilgi teminatı cyber defence, intelligence, operations info sec compu sec , information assurance vs.

1) Cybersecurity: Definition of cybersecurity in the dictionary,"the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this" [2]

To understand the term cybersecurity we must first define the term cyberrisk.

Cyberrisk is not one specific risk. It is a group of risks, which differ in technology, attack vectors, means, etc. We address these risks as a group largely due to two similar characteristics: A) they all have a potential great impact B) they were all once considered improbable. [3]

2) Cyberrisk: Cybersecurity is the sum of efforts invested in addressing cyberrisk, much of which was, until recently, considered so improbable that it hardly required our attention.

XXX Cyberrisk kurumlar için de geçerli..

3) Cyberdefence:

4) CyberOperations:

B. Development of Cyber Security

Mevcut süreçler, ISO 27001, BSYG vb. , klısımda uluslaraso ve ülke bazı oluştır ihtiçi

1) From Information Security to Cyber Security:

2) A New Concept Institutional Cyber Security: * Enforcement of cyber security rules and policies must be met by the institutions and auditing should be taken into consideration whether the institutions comply with given set of cyber security policies. Institutions should not have a choice not to be a part of cyber security enforcement process (Needs to be defined).

* The terms of INFOSEC and COMPUSEC are not providing cyber security needs of the institutions. Altough protecting institutional data, providing business continuity and so forth, The Process of Information Security Management fails to envision, deter, mitigate or prevent some large scale and targetted malwares like fatmall, duqu, stuxnet, and so forth that in other terms what we call Advanced Persistant Threats. (Brief info about APT can be given here)

grafik çiz.

The ITU also defined cyber security broadly as:'[T]he 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. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality.'Many countries are defining what they mean by cyber security in their respective national strategy documents. [4] 1.4.1. The Three Dimensions: Governmental, National and International

Any approach to a NCS strategy needs to consider the 'three dimensions' of activity: the governmental, the national (or societal) and the international. Since the 1990s a particular trend in public policy theory has focused on the cooperation of different actors. Initially the focus was on improving the coordination of government actors (the Whole of Government approach or WoG), particularly between the departments most involved in stabilisation or peace building operations in places like Afghanistan or Iraq.

To follow a cyber security roadmap is crucial for the critical infrastructures like telecomunications, transportation, health sectors and so forth that form essence and is part of national security (Referans, Bilge Hoca'nın Makalesi) other governmental sectors like agriculture, forestry that may seem less important in terms of being a criical infrastructure, , non governmental and private sectors are also inevitably need to track a cyber security roadmap.

C. DILEMMAS OF NATIONAL CYBER SECURITY

THE FIVE DILEMMAS OF NATIONAL CYBER SECURITY 1.5.1. Stimulate the Economy vs. Improve National Security 1.5.2. Infrastructure Modernisation vs. Critical Infrastructure Protection 1.5.3. Private Sector vs. Public Sector 1.5.4. Data Protection vs. Information Sharing 1.5.5. Freedom of Expression vs. Political Stability [4] XXX Buradaki ikilemlerden 1 cümle ile değerlendirme kısmında ya da policy kısmında değinilebilir.

D. Challenges

While the weakest chain in security is human being, in terms of national security the weakest chain is the weakest institution having critical infrastructures.

Challenges - Legal - Leadership - Cost - Lack of trained personnel, human resource

Migration plan XXX Outsurcing mi in home development mı? IT security professionals said that outsourcing would be the biggest cybersecurity threat

IV. INSTITUTIONAL CYBER SECURITY ROADMAP

Ulusal/kurumsal yol haritası Yapılacakların özeti

A. Significance of Roadmapping

* The significance of this work is to fill the absence of such kind of roadmaps and guidelines dedicated solely to institutions.

[1] Numarlı kaynaktan alınabilecek husular The United States is at a significant decision point. We must continue to defend our current systems and networks and at the same time attempt to "get out in front" of our adversaries and ensure that future generations of technology will position us to better protect our critical infrastructures and respond to attacks from our adversaries. are much more resilient.

The R&D investments recommended in this roadmap must tackle the vulnerabilities of today and envision those of the future.

11 hard problems on cyber security of countries. XXX Burada ABD kendisi ve ülkeler için zor problem olan sahaları /araştırma alanlarını sıralamış bu sahaların kurumlar için olanlar listelenebilir ve bu listelenen problemleri çözmeye aday bir yol haritası sunuyoruz diyebiliriz. Each of the following topic areas is treated in detail in a subsequent section of its own, from Section 1 to Section 11. 1. Scalable trustworthy systems (including system architectures and requisite development methodology) 2. Enterprise-level metrics (including measures of overall system trustworthiness) 3. System evaluation life cycle (including approaches for sufficient assurance) 4. Combatting insider threats 5. Combatting malware and botnets 6. Global-scale identity management 7. Survivability of time-critical systems 8. Situational understanding and attack attribution 9. Provenance (relating to information, systems, and hardware) 10.Privacy-aware security 11.Usable security

[1]

Why an institution neeeds a road map?

B. Methodology

The methodology for development an cyber security roadmap is similar to technology roadmapping because cyberspace grows/changes/develop fast like technological devepments. The methodology for development an cyber security roadmap consist of three phases: preliminary activity, development of the roadmap and follow-up activity. [1]

In the Phase I. Preliminary activity 1. Satisfy essential conditions. 3. Define the scope and boundaries for the roadmap.

Phase II. Development of the Roadmap 1. Identify the "cyber security issues" that will be the focus of the roadmap. 2. Identify the critical cyber security requirements and their targets. 3. Specify the major cyber security areas. 4. Specify the cyber security drivers and their targets. 6. Recommend the technology alternatives that should be pursued.

Phase III. Follow-up activity 1. Critique and validate the roadmap. 2. Develop an implementation plan.

Makale de bulunmasını isteğimiz sahalar The identification and description of each technology area and its current status. • Critical factors (show-stoppers) which if not met will cause the roadmap to fail. • Areas not addressed in the roadmap. • Technical recommendations. • Implementation recommendations.

C. XXX

1) Security perception & Awareness: * The relation between habits and security perception should be probed among individuals especially among system administrators.

2) XXX: At both the individual corporate and industry levels, technology roadmapping has several potential uses and resulting benefits. Three major uses are: • First, technology roadmapping can help develop a consensus about a set of needs and the technologies required to satisfy those needs. • Second, it provides a mechanism to help experts forecast technology developments in targeted areas. • Third, it can provide a framework to help plan and coordinate technology developments both within a company or an entire industry.[51] XXX restament

XXX 2 tür Roadmapping var .. biz bir tanesiinin üzerinden gidelim This roadmapping consists of three phases: 1. Assessment (i.e., establish assumption, establish regulatory requirements, establish committed milestones, depict logics and planned activities). 2. Analysis (i.e., identify issues, perform root-cause analysis, and translate issues to activities). 3. Resolution (develop issue-resolution documents and integrate activities with activity data sheets). Although there are some similarities, this roadmapping approach is fundamentally different (in purpose, scope, and steps) from the technology roadmapping process addressed by this paper. [5]

XXX 1 numaralı kaynağımızda research için bir yol haritası derken kısa orta ve uzun vadede neler yapılabileğini listelemiş.. ve milestonelar sıralamış Bizimki Roadmap olacaksa bizdede bu tür bir tasnif gerekli. 1. kaynakta her bir problem için TABLE 1.1: Summary of Gaps, Approaches, and Benefits isimli tablolarda sorunlar özetleniyor.. bunlardan kurumsal olanları süzebiliriz. [1]

V. Conclusion

Burada başarılı olmak için gerekli olana ilave hususlar vs. eklenebilir. Bizim yeniliğimiz 1. devlet kurumları ve büyük ölçekli firmalar için kurumsal yol haritası olması 2. Reccomendation Bizim yol haritası kendileri için yol haritası hazırlamak isteyen kurumlar için genelbir yol.har. Kuurumlar yapılarına durumlarına özel mutlaka daha detay lı yh.ları hazırlamalısırlar.

Appendix A
Proof of the First Zonklar Equation

Appendix one text goes here.

Appendix B

Appendix two text goes here.

Acknowledgment

The authors would like to thank Turkish Armed Forces Cyber Defence Center staff.

References

[1] D. Maughan *et al.*, "A roadmap for cybersecurity research," *US Department of Homeland SecurityNovember*, vol. 2009, 2009.
[2] (2013, Jun.) Oxford dictionaries. [Online]. Available: http://oxforddictionaries.com/
[3] M. Barzilay. (2013, May) A simple definition of cybersecurity. [Online]. Available: http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296
[4] U. Kurt, "Cyber security: A road map for turkey," DTIC Document, Tech. Rep., 2012.
[5] M. L. Garcia and O. H. Bray, *Fundamentals of technology roadmapping*. Sandia National Laboratories Albuquerque, NM, 1997.

Michael Shell Biography text here.

John Doe Biography text here.

Jane Doe Biography text here.