ÇEŞİTLİ ÜLKELERDE USOM ve SOME YAPILANDIRILMASI
ve
TÜRKİYE MODELİ ÖNERİSİ

Sinem Sanalp
114691003

İSTANBUL BİLGİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

Prof. Dr. Ahmet DENKER

2016

ÇEŞİTLİ ÜLKELERDE USOM VE SOME YAPILANDIRILMASI
VE
TÜRKİYE MODELİ ÖNERİSİ

CYBER SECURITY STRUCTURES IN VARIOUS COUNTRIES
AND
PROPOSAL OF TURKEY MODEL

Sinem SANALP
114691003

Prof. Dr. Ahmet DENKER	:	
Doç. Dr. Leyla KESER BERBER	:	
Yrd. Doç. Dr. Mehmet Bedii KAYA	:	
Tezin Onaylandığı Tarih	:	
Toplam Sayfa Sayısı	:	73

Anahtar Kelimeler (Türkçe)	Anahtar Kelimeler (İngilizce)
1) Siber Güvenlik	1) Cyber Security
2) Siber Uzay	2) Cyber Space
3) Siber Ordu	3) Cyber Army
4) Kritik Altyapı	4) Critical Infrastructure
5) Veri Güvenliği	5) Data Security

Özet

Teknoloji ve internet, gündelik hayatın vazgeçilmez bir unsuru haline gelmiş ve günümüzde internet erişimi, birçok sektör için elzem olmuştur. Siber saldırıların muhtemel etkileri büyük olacağından; sistemlerin olası saldırılardan korunması, üzerinde düşünülmesi gereken bir konu haline gelmiştir. Dolayısıyla siber güvenlik, ülkelerin savunmasında yeni bir aktör olarak nitelendirilmeye başlanmıştır ve birçok ülke, kamu ve özel sektörde siber savunma alanında ciddi adımlar atmaktadır. Bu çalışmada, siber güvenlik ve siber savunma alanında başarılı olan ülkelerin, yürüttükleri çalışmalar ile ulusal siber savunma yapıları incelenmiş; bu örnekler ışığında ülkemizin siber güvenlik yapılanması için önerilerde bulunulmuştur. Çalışma kapsamında, öncelikle Türkiye'nin siber güvenlik alanındaki mevcut durumu incelenmiştir. Sonrasında, örnek siber güvenlik uygulamaları, siber güvenlikten sorumlu kurumların organizasyonu, kritik altyapıların siber güvenliğinin sağlanması, atılması gereken adımlar, siber güvenlik iş gücünün temini, gelecek nesil teknolojilerin siber güvenliği gibi konularda inceleme ve önerilere yer verilmiştir.

Abstract

Technology and internet are an unforgettable thing for daily life and communication of internet is an advantage for lots of sectors.Because of serious effects of cyber attacks being protected of systems from these attacks is an important issue.So,cyber security is seen as a new actor for being protected from these attacks.That's why a lot of country is trying to improve for the cyber defence of some of sectors and civil.In that study works which are being examined of developed countries at the field of cyber safety and cyber defency are examined; with the examples of these studies a lot of suggestions are presented for our country's cyber safety.In that work Turkey's normal condition at the field of cyber defency is examined and then serious topics like cyber safety applications, organisation of cyber safety,being provided of critic infrastructure of cyber safety,making sure of cyber safety and cyber technology of next generations are examined and begin to give place for the suggestions.

Önsöz

Bu çalışmanın hayata geçirilmesi aşamasında değerli katkılarını esirgemeyen Prof. Dr. Ahmet Denker, Doç. Dr. Leyla Keser Berber, Yrd. Doç. Dr. Mehmet Bedii Kaya ve Dr. Tayfun Acarer'e ayrıca çalışma boyunca manevi desteklerini her an hissettiğim aileme teşekkürlerimi sunarım.

İÇİNDEKİLER

KISALTMALAR

ABD	:	Amerika Birleşik Devletleri
ADSL	:	Asymmetric Digital Subscriber Line
ANSSI	:	Agence nationale de la sécurité dessystèmes d'Information
BİLGEM	:	Bilgi ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BSI	:	German Federal Office for Information Security
BTK	:	Bilgi Teknolojileri ve İletişim Kurumu
C4I	:	Command, Control, Communications, Computers and Intelligence
CCD-COE	:	Cooperative Cyber Defence Centre of Excellence
CDMA	:	Cyber Defense Management Authority
CEO	:	Chief Executive Officer
CERC	:	Cyber Security Education and Research Centre
CERT	:	Computer Emergency Response Team
CERT-EE	:	Computer Emergency Response Team Estonia
CIA	:	Central Intelligence Agency
CIIP	:	Department of Critical Information Infrastructure Protection
CNCI	:	Comprehensive National Cybersecurity Initiative
CPNI	:	Center for Protection of National Infrastructure
DDos	:	Distributed Denial of Service Attack
DIA	:	Defence Intelligence Agency
DMI	:	Directorate of Military Intelligence
DNS	:	Domain Name System
DOJ	:	Department of Justice
DSH	:	Department of Homeland Security
DSL	:	Digital Subscriber Line
EISA	:	Estonian Information Systems Authority
FBI	:	Federal Bureau of Investigation
FSB	:	Russian Federal Security Service
G8	:	Group of Eight
GCHQ	:	Government Communications Headquarters
GPRS	:	General Packet Radio Service
GSM	:	Global System for Mobile Communications
GSS	:	General Security Service of Israel
HAVELSAN	:	Hava Elektronik Sanayii
IAI	:	Israil AeroSpaces Industries
IBM	:	International Business Machines
ICP	:	Internet Content Provider
IDF	:	Israil Defence Forces
IOT	:	Internet of Things
IP	:	Internet Protokol
ISTF	:	Information Security Task Force
IT	:	Information technology
M2M	:	Machine to Machine
MLPS	:	The Multi-Level Protection Scheme
NATO	:	North Atlantic Treaty Organization
NCA	:	National Crime Agency
NCCIC	:	National Cybersecurity and Communications Integration Center
NICCS	:	National Initiative for Cybersecurity Careers and Studies
NICE	:	National Iniative for Cybersecurity Education

NSA	:	National Security Agency
NSC	:	National Safety Council
NSD	:	National Security Database
OSCE	:	The Organization for Security and Co-operation in Europe
PCII	:	Protected Critical Infrastructure Information
PLA	:	People's Liberation Army
RF	:	Radio frequency
RTU	:	Remote Terminal Unit
SCADA	:	Supervisory Control and Data Acquisition
SGE	:	Siber Güvenlik Enstitüsü
SOME	:	Siber Olaylara Müdahale Ekibi
TDK	:	Türk Dil Kurumu
TIC	:	Trusted Internet Connections
TİB	:	Telekomünikasyon İletişim Başkanlığı
TSK	:	Türk Silahlı Kuvvetleri
TÜBİTAK	:	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UHDB	:	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
URL	:	Uniform Resource Locator
USOM	:	Ulusal Siber Olaylara Müdahale Merkezi
3G	:	3rd Generation

KAYNAKÇA

1. 2016-2019 Ulusal Siber Güvenlik Stratejisi
2. Goodwin, Cristin Flynn, Nicholas, J. Paul. "Developing a National Strategy for Cybersecurity" (2013, Ekim)
3. Locasto, Michael E., Ghosh, Anup K., Jajodia, Sushil, Stavrou, Angelos. "The Ephemeral Legion: Producing an Expert Cyber Security Work Force From Thin Air". (2011, Ocak). Doi:10.1145/1866739.1866764
4. USOM-TR CERT. "Siber Güvenliğe İlişkin Temel Bilgiler" (2014, Temmuz). Erişim tarihi: 01.12.2016.
5. Ünver, Mustafa, Canbay, Cafer, Mirzaoğlu, Ayşegül. "Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler" (2009, Mayıs)
6. Yıldız, Mithat. "Siber Suçlar ve Kurum Güvenliği"(2014 Kasim).
7. CCDCOE. "Cyber Security Strategy Documents" (2015 Ekim). Erişim tarihi: 10.11.2015. https://ccdcoe.org/cyber-security-strategy-documents.html
8. Tabansky, Lior. "Cyberdefence Policy oof Israel: Evolving Threats and Responses" (2013, Ocak)
9. Ferwerda, J., Choucri, N., Madnick, S. "Institutional Foundations for Cyber Security: Current Responses and New Challenges" (2010, 19 Mart)
10. Bakır, Emre. "5. Boyutta Sacaş: Siber Savaşlar – I" (2012, 20 Aralık). Erişim tarihi:21.12.2015. https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-i.html
11. Bakır, Emre. "5. Boyutta Sacaş: Siber Savaşlar – II" (2012, 2 Ocak). Erişim tarihi:21.12.2015. https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-ii.html
12. Singer, P. W., Friedman, Allan. "Siber Güvenlik ve Siber Savaş" (Çev. Ali Atav). Ankara, 2015
13. Baram, Gil. "The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case" (2013, Mayıs). Military and Strategic Affairs
14. İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü. "Siber Güvenlik Raporu" (2012, Mayıs), Erişim tarihi:10.11.2015.
15. Prescott, Jody M.. "Building the Ethical Cyber Commander and the Law of Armed Conflict"(2014)
16. Reed, John. "Unit 8200: Israel's cyber spy agency" (2015, 10 Temmuz). Erişim tarihi: 18.11.2015. http://www.ft.com/cms/s/2/69f150da-25b8-11e5-bd83-71cb60e8f08c.html
17. Kumar, Mukherjee. "Cyber Security in India: A Skill Devolopment Perspective" (2013)
18. Anonim. "Cyber Security Jobs in India are Making a Comeback!" (2014, Şubat). Digital Learning
19. "Sardıç: ABD Siber Ordu için Silikon Vadisi ile Çalışıyor" (2015, 14 Eylül). Erişim tarihi: 02.01.20.16.
20. Payne, Robert W.. "Departing Employees and 'Abandoned' Research" (2016, Ocak). The Computer & Internet Lawyer
21. Anonim. "Public Sector IT Suppliers must meet Cyber Essentials Scheme Regulations"(2014 Ekim). Computerweekly.com
22. Lifland, Amy. "The Future of Conflicts"(2012 Bahar Dönemi). Global Notebook
23. Anonim. "Siber Güvenlik Ulusu: İsrail Ağı Korumada Nasıl Dünya Lideri Oldu" (2014, 22 Aralık). Erişim tarihi: 01.12.2015. http://itrade.gov.il/turkey/siber-guvenlik-ulusu-israil-agi-korumada-nasil-dunya-lideri-oldu/#sthash.8FFWSktV.dpuf
24. Ehrenreich, Daniel. "Attacking SCADA Systems of Critical Infrastructure" (2015, 1 Kasım). Erişim tarihi: 1.12.2015. http://www.israeldefense.co.il/en/content/attacking-scada-systems-critical-infrastructure
25. Çelik, Minhac. "States' Relations with Non-State Groups in Cyberspace" (2014 Kasım)

26. Atalay, Ahmet Hamdi. "Siber Suçlar ve Siber Savaşlar". (203 Mayıs). Erişim tarihi: 02.12.2015. http://www.bilgiguvenligi.org.tr/s/2246/i/siber_guvenlik_itgsc-aha-istanbul-mayis-2013.pdf

27. China Monitor. "Cyber Security in China: New Political Leadership Focuses on Boosting National Security" (2014, Aralık). Erişim Tarihi: 05.12.2015. http://www.merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf

28. Watts, Jonathan. "Gmail hack: phishing finger pointed at China's Lanxiang vocational school" (2011, 2 Haziran). Erişim tarihi: 10.12.2015. http://www.theguardian.com/technology/2011/jun/02/chinese-school-implicated-cyber-attacks

29. Chaturvedi, M. M., Gupta, MP, Bhattacharya, Jaijit. "Cyber Security Infrastructure in India: A Study". Erişim tarihi: 11.12.2015. http://www.iceg.net/2008/books/2/9_70-84.pdf

30. https://nsa.gov1.info/surveillance/

31. Yener, Yavuz. "Rus Krizinin Gözden Kaçan Boyutu: Siber Savaş Tehdidi" (2015, 2 Aralık). Erişim tarihi: 10.12.2015. http://www.usak.org.tr/analiz_det.php?id=17&cat=365366706#.VofHRPkaaT9

32. "Yeni Tehditler: Siber Boyut" Erişim tarihi: 10.12.2015. http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/TR/

33. Yener, Yavuz, "NATO ve Siber Güvenlik 2 – Strateji" (2014, 27 Aralık). Erişim tarihi: 11.12.2015. http://siberbulten.com/makale-analiz/nato-ve-siber-guvenlik-2-strateji/

34. Ulmer, Kathrin. "Cyber Risks and Cyber Security – Risk Communication and Regulation Strategies in the U.S. and Germany" (2014, 2 Haziran)

35. Anonim. "Cyber Security in India". Erişim tarihi: 03.01.2016. http://cybersecurityforindia.blogspot.com.tr/

36. Şumlu, Selim. "Hacker'ın Uyanışı" (2013 Mart). PC Net

37. Estonian Defence League. "Cyber Defence Unit". (2015, 3 Ağustos). Erişim tarihi: 12.12.2015. http://www.eesti.ee/eng/topics/riigikaitse/vabatahtlik_osalemine_riigikaitses/kuberkaitse_uksus

38. Anonim. "Cyber Security Status Watch"(2013)

39. Bozdemir, Nazlı Zeynep. "İngiltere'yi Siber Güvenlik Sektöründe Sırtlayan Adam"(2014, 8 Aralık). Erişim tarihi: 12.12.2015. http://siberbulten.com/makale-analiz/ingiltereyi-siber-guvenlik-sektorunde-sirtlayan-adam-andy-williams/

40. "İngiliz üniversiteleri siber savaşçı yetiştirmek için kolları sıvadı" (205, 4 Temmuz). Erişim tarihi: 15.12.2015. http://siberbulten.org/strateji-guvenlik/ingiliz-universiteleri-siber-savasci-yetistirmek-icin-kollari-sivadi/

41. http://siberbulten.com/uluslararasi-iliskiler/abd/amerikanin-kriptologlarini-yetistiren-gizli-okulun-hikayesi/?utm_content=buffer40b2d&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer

42. Güngör, Murat. "Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma" (2015, Mart)

43. http://www.dhs.gov/einstein

44. http://www.internetkurulu.org/tr/SGInsiyatifi.aspx

45. https://en.wikipedia.org/wiki/Golden_Shield_Project

46. Anonim. "Zetta-Byte'ın Yılı" (2016 Ocak). Popular Science

47. Atikkan, Zeynep, Tunç, Aslı. "Blogdan Al Haberi". İstanbul, 2011

48. Kara, Mehmet, Çelikkol, Soner. "Ağ ve Bilgi Güvenliği Sempozyumu-Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği". (2011)

49. Karakuş, Cahit. "Kritik Alt Yapılara Siber Saldırı"

50. https://tr.wikipedia.org/wiki/H%C3%BCk%C3%BCmet_i%CC%87leti%C5%9Fim_merkezi

51. http://siberbulten.com/strateji-guvenlik/ingiltereden-kobiler-icin-siber-guvenlik-destegi/

52. Pwc. "2015 Information Security Breaches Survey" (2015)

53. http://siberbulten.org/strateji-guvenlik/ingiliz-universiteleri-siber-savasci-yetistirmek-icin-kollari-sivadi/

54. Atalay, Ahmet Hamdi. "Siber Evrende Güvenlik" (2014, 10 Eylül). Erişim tarihi: 30.12.2015. http://bilgicagi.com/siber-evrende-guvenlik-3/

55. Davulcu, Buket. "Sanal dünyada gerçek savaş: Siber saldırılar" (2014, 6 Ocak). Erişim tarihi: 18.12.2015. http://www.aksiyon.com.tr/kapak/sanal-dunyada-gercek-savas-siber-saldirilar_537462

56. Gedik, Muhammet. "Siber Uzay, Uluslararası Hukuk ve Türkiye" (2015, 5 Aralık). Erişim tarihi: 10.12.2015. http://h4cktimes.com/analiz-makaleler/siber-uzay-uluslararasi-hukuk-ve-turkiye.html

57. Yazıcı Altıntaş, Emine. "Ulusal Siber Güvenlik Çalışmaları ve Kurumsal SOME'lerin İşleyisi". Erişim tarihi: 04.04.2016. https://www.usom.gov.tr/faydali-dokuman/15.html

58. Anonim. "Siber Güvenlik - Siber Saldırılar – Bilgi Güvenliği".(2014, 18 Mayıs). Erişim tarihi: 19.12.2015. http://www.isfikirleri-girisimcilik.com/siber-guvenlik-siber-saldirilar-bilgi-guvenligi

59. Bozdemir, Nazlı. "Türkiye ve Siber Güvenlik: Tehditlerin Farkında mıyız?" (2013, 21 Temmuz). Erişim tarihi: 28.12.2015. http://akademikperspektif.com/2013/07/21/turkiye-ve-siber-guvenlik-tehditlerin-farkinda-miyiz-3/

60. Kırdı, Gökhan. "Türkiye'de ve Dünya'da Siber Güvenlik Alanında Yapılan Çalışmalar" (2015, 14 Ocak). Erişim tarihi: 01.12.2015. http://sahipkiran.org/2015/01/14/siber-guvenlik/

61. Yap, Gerald T., Major, USA. "Sovereign State's Options if Attacked in Cyberspace: A Case Study of Estonia 2007" (2009 Nisan)

62. "Information System Defence and Security- France's Strategy" (2011, 15 Şubat). Erişim tarihi: 15.12.2015

63. Benoliel, Daniel. "Towards a Cyber Security Policy Model: Israel National Cyber Bureau (INCB) Case Study" (2014, Haziran)

64. Anonim. "Siber Suçlar Çocuk Oyuncağı Oldu" (2016, 3 Ocak). Erişim tarihi: 04.01.2016. http://siberbulten.com/strateji-guvenlik/siber-suclar-cocuk-oyuncagi-oldu/

65. Orijinal çizim için bknz. USOM, USOM Faaliyetleri. Erişim tarihi: 04.04.2016. https://www.usom.gov.tr/faydali-dokuman/15.html

66. Türkiye Bilişim Derneği. "Siber Güvenlik ve Kritik Altyapı Güvenliği Çalışma Grubu Nihai Rapor"(2015, 5 Ekim).

67. http://sge.bilgem.tubitak.gov.tr/

68. https://www.dhs.gov/critical-infrastructure-security-resilience-month

ŞEKİLLER

TABLOLAR

Çeşitli Ülkelerde USOM ve SOME Modeli ve Türkiye Modeli Önerisi

1. Giriş

Teknolojinin ve internetin gelişimine paralel olarak gündelik hayatta kullandığımız sistemlerden, devletlerin savunma sistemlerine kadar her alan büyük bir değişim ve gelişim içindedir. Devlet kurumlarının, işlemleri dijital sistemler üzerinden yapmaya başlaması, bilgisayar sistemlerinin ve internetin bankacılık, finans, telekomünikasyon gibi sektörler için olmazsa olmaz hale gelmesi; ancak bu sistemlerin güvenliğinin aynı hızda sağlanamaması büyük sorunlara sebep olmuştur ve hala geleceğin en büyük sorunlarından biri olarak ifade edilmektedir. Örneğin İngiltere'nin en büyük beş bankası siber güvenlik konusunu en büyük önceliğe sahip konu olarak görmektedir ve önemli şirketlerin CEO'larının en endişelendiği konu, yine siber güvenlik konusudur. Bunun birden çok sebebi bulunmaktadır. Öncelikle şirketler, tüm sistemin mevcut açıklarını bulup önlem almak zorundadır. Oysa saldırganlar, belli bir noktaya yoğunlaşıp, açık bulabilmektedir. Ayrıca bir şirketin sistemlerinin güvenliğini sağlamak oldukça maliyetli olabiliyorken, saldırı düzenlemek için büyük meblağlar gerekmemektedir. Hem de zombi[1] bilgisayarların kullanılması nedeniyle suçluyu bulmak neredeyse imkansızdır.

Siber saldırı denince akla ilk gelenler, devlet kurumlarına ait sistemlere veya bankalara yapılabilecek saldırılar olmaktadır. Devlet kurumlarına yapılan saldırılar, daha çok siber aktivizim veya siber savaş türünde olmaktadır. Siber aktivistler, "dünya görüşleri çerçevesinde kötü veya uygunsuz gördükleri toplumsal ya da politik sorunları dile getirmek amacı ile kamu ya da özel sektör siber uzaylarına saldırı düzenleyen şahıs ya da gruplardır."[2]Siber savaş ise "Siber uzayı ve içindeki varlıkları korumak için yürütülen harekatların geneline verilen

[1]Saldırganların, hacking yoluyla ele geçirdiği ve yaptığı sanal saldırılarda maske olarak kullandığı bilgisayarlara verilen isim.
[2]USOM-TR CERT. "Siber Güvenliğe İlişkin Temel Bilgiler" (2014, Temmuz). Erişim tarihi: 01.12.2016.

isimdir."[3]Banka, özel şirket gibi kurumlara yapılan saldırılar ise maddi hırsızlık veya bilgi hırsızlığı amacıyla olabilmektedir.Bununla birlikte, son zamanlarda devlet kurumlarının özel sektör şirketlerine saldırı düzenlediği olaylar da olmaya başlamıştır. Burada amaç, özel sektördeki teknik bilgilerin çalınması veya siber güvenlik alanında özel sektör ile ortak çalışmalar yürüten ülkelerde, dolaylı olarak ülkelere saldırmak olabilmektedir. Ne var ki; siber saldırıların amaç ve araçlarının bu kadar çeşitlendiği bir ortamda, ülkelerin siber güvenlik konusunda ciddi çalışmalar içine girmesine sebep olan faktör, bunların hiçbiri değildir. Ülkelerin bilgi ve sistem güvenliğinin ne kadar önemli olduğunu fark etmesine Estonya'da yaşanan ve günlerce tüm sistemleri kilitleyen siber saldırı ve 2013 yılında yaşanan, Edward Snowden'ın ABD Ulusal Güvenlik Ajansı NSA'nın sistemlerine sızarak, ticari ve diplomatik birçok belgeyi ele geçirmesi olayı sebep olmuştur. Bu iki olay, siber güvenlik alanında milat olmuştur ve ülkeler, iletişim sistemlerini ve altyapısını her türlü tehlikeden korumak zorunda olduklarını yaşayarak öğrenmişlerdir. Bu noktada, devletlerin siber güvenlik konusuna bakışı ile kurumların görev ve yetkileri ile kurumlar arası iletişim ve çalışma şeklinin belirlenmesi; siber güvenlik uzmanlarının yetiştirilmesi gibi birçok konuda çeşitli fikirler üretilmiştir ve üretilmeye devam etmektedir. Son yıllarda birçok ülke, siber güvenliğe ayırdığı bütçeyi kat be kat artırmıştır.[4] Sadece bu bilgi bile, siber güvenlik alanındaki çalışmaların ne kadar elzem olduğunu kanıtlar niteliktedir.

Bu çalışmada, siber güvenlik konusunda çalışmalar yapan ve kurumlarını belli bir noktaya getirmiş belli başlı ülkelerin siber güvenlik stratejileri, kullandıkları yöntemler, çalışma biçimleri, USOM ve SOME yapıları incelenecek; tüm ülkelerin sistemlerinin iyi ve kötü yönleri ışığında Türkiye için USOM ve SOME modeli önerisi sunulacaktır.

[3]Bakır, Emre. "5. Boyutta Sacaş: Siber Savaşlar – I" (2012, 20 Aralık). Erişim tarihi:21.12.2015. https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-i.html

[4]https://siberbulten.com/sektorel/siber-guvenlik-harcamalari-170-milyar-olacak-en-hizli-g-amerika-buyuyecek/

2. Ülkelerin İncelenmesi

I. Amerika Birleşik Devletleri ve Siber Güvenlik Uygulamaları

Amerika Birleşik Devletleri, siber güvenlik konusunda aldığı aksiyonlar ve siber uzay kavramının oluşmasına verdiği destek ile öne çıkmaktadır. Devlet içinde oturmuş ve çerçevesi çizilmiş bir siber güvenlik yapılanması bulunmaktadır. Ülkede hem kurumların görev ve yetkileri tam olarak belli hem de bu iş için verilen çabalar düzenli olarak devam etmekte, gelişen teknolojiye uyum sağlanmaktadır. ABD, düzenli aralıklarla güvenli siber uzay için ulusal stratejilerini güncellemekte, yeni hedefler belirlemekte ve bu stratejileri toplum ile paylaşmaktadır.

ABD, bugüne kadar yaptığı çalışmalar ile siber güvenlik sistemini geliştirmiştir. Siber güvenlik stratejilerinin ilk oluşturulduğu yıllarda yazılan raporlarda, güvenlik ile ilgili sorumluluğu olan birçok kurumun olduğu ve hangi kurumun yetkisinin nerde başlayıp nerede bittiğinin tam olarak belli olmadığı bununla birlikte hiçbir kurumun da karar verme ve uygulama yetkisine sahip olmadığı belirtilmektedir. ABD, 2006 yılına kadar güvenliğini büyük ölçüde özel sektöre ve CERT/CC kurumuna emanet etmiştir. Ayrıca ordu da kendi içinde kendi siber güvenliğini sağlamıştır ancak teknolojinin gelişimi ile paralel olarak koruma yöntemlerinin güncellenememesi sonucunda 2006 yılında "Wikileaks Belgeleri" olayı yaşanmıştır. Bahsedilen olay, Julian Assenge ismindeki bir hackerın ABD'nin güvenlik konusundaki en önemli birimi olan Ulusal Güvenlik Ajanjsı (NSA)'nın sistemlerine sızıp birçok gizli belgeyi ele geçirmesi ve kurduğu Wikileaks adlı internet sitesinde ifşa etmesi olayıdır. Bu saldırılara karşılık olarak söz konusu siteye, erişimin engellenmesi amacıyla, DDoS saldırıları gerçekleştirilmiş; bu DDoS saldırılarına karşılık olarak da hacker gruplardan biri, Mastercard, Paybal, Visa ve çeşitli devlet kurumlarını hedef alan saldırılar başlatmıştır. Bu olay aslında hem ABD için hem de diğer ülkeler için siber güvenlik konusunda milat olarak kabul edilen olaylardan biridir. Wikileaks, siber uzayın bizim veri ve erişim ile olan ilişkimizi nasıl radikal bir şekilde değiştirdiğini anlamak için bir odak noktasına dönüşmüştür.[5] ABD yönetimi, bunu doğrular şekilde söz konusuolaydan sonra internet politikalarını gözden geçirmiş

[5]Singer, P. W., Friedman, Allan. "Siber Güvenlik ve Siber Savaş" (Çev. Ali Atav). Ankara, 2015

ve önemli kararlar almıştır. Bu kararlara göre siber güvenlik konusundaki tüm sorululuk DSH (Department of Homeland Security)'a verilmiştir. Bu kurum altında hizmet vermek üzere ulusal CERT organizasyonu (US-CERT) oluşturulmuştur. Wikileaks belgelerinin ifşa edilmesi olayı, aynı zamanda karşılıklı saldırıların yapıldığı ilk sanal savaşlardan biri olarak nitelendirilebilir.

US-CERT, DSH kurumunun Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (NCCIC) birimi altında görev yapan bir daldır. Görev tanımı, ulusal siber güvenliği sağlamak, siber güvenlik için bilgi paylaşımını koordine etmek ve proaktif risk yönetimi olarak belirtilir. 7x24 çalışma prensibi ile sistem operatorlerine destek sağlamak ve güvenlikle ilgili olayları takip etmekten sorumlu birimdir. Çalışma şeklindeki en dikkat çekici taraf, internet sitesinden form doldurularak siber güvenlikle ilgili saldırıların anından kuruma bildirilebilmesidir. Üstelik bildirimlerin siber saldırı ve yazılım açığı olarak ayrıştırılması da mümkün olmaktadır.

US-CERT, Korunan Kritik Alt Yapı Bilgisi (PCII) programını finanse etmektedir. Bu program, hassas veri ve uygun olmayan özel bilgileri korumayı hedeflemektedir. Oluşturulan bu sistem, özel sektör üyelerinin sistemlerine ait veriyi, verinin güvenliğinden emin olduğu için, devlet kurumlarına gönül rahatlığı ile vermesini sağlamaktadır. PCII programı, sistemlerin güvenliğini sağlar ve kritik bilgiyi analiz eder; sistemlerdeki güvenlik açıklarını belirler ve risk analizi yapar; herhangi bir veri kaybı durumu ihtimaline karşı veri kurtarma için hazırlık yapar. PCII, kritik verinin korunmasını kritik verileri baz alarak kaza/saldırı müdahale planları oluşturma, bilgisayar sistemlerini sistem güvenliği açısından analiz etme, binanın fiziksel açıklarını tespit etme şeklindeki aksiyonlar ile sağlamaktadır. Kişisel ve hassas bilgiler, PCII programı kapsamında kanunlar ile koruma altına alındığı için bilgi paylaşımı konusunda şirketlerin endişe duymadığı belirtilmektedir.

ABD'de 2008 yılında yeni bir streteji planı çerçevesinde Kapsamlı Ulusal Siber Güvenlik Girişimi (CNCI) direktifi hazırlanmıştır ve dönemin başkanı George W. Bush tarafından imzalanmıştır. Bu direktif daha sonraki yıllarda da güncellenerek kullanılmaya devam etmiştir. Bu dokümanda yer alan önemli maddeler,

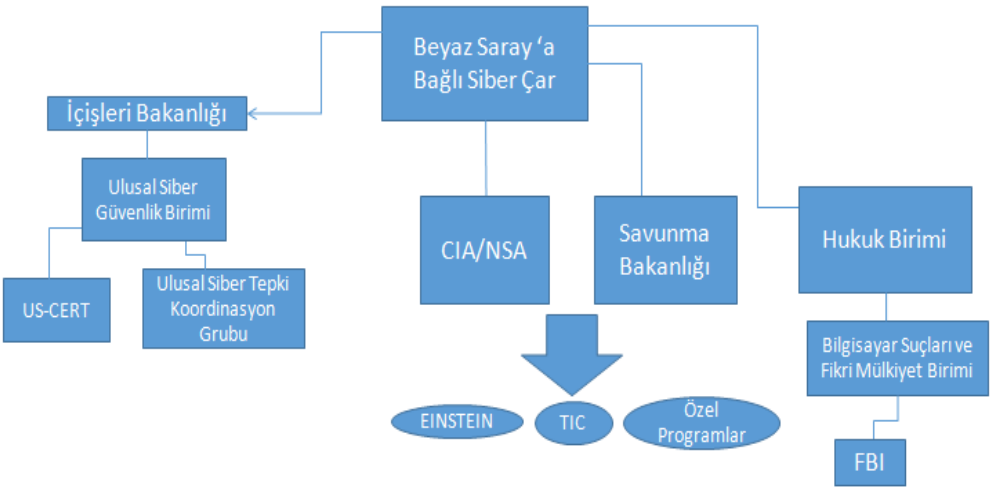
- Devlet kurumları ile dış kurumlar arasındaki ağ bağlantılarının sayısının azaltılması,

- DSH bünyesinde kullanılan EINSTEIN programının kullanım yetkisinin NSA birimine (ulusal güvenlik birimi) aktarılması. Bu programın yeni versiyonunda web trafiğini izlemenin yanındaiçeriğini de izleme özelliği yer alıyordu.Tabii bu durum özel hayatın gizliliği noktasında tartışmalara açık bir durumdur,
- Siber güvenlik için araştırma ve geliştirme çalışmalarının artırılması,
- Siber güvenlikle ilgili istihbarat çalışmalarının koordinasyonunun sağlanması,
- Hükümetin kurumları arasındaki bilgi paylaşımının sağlanması,

olarak sıralanabilir.

Barack Obama döneminde belgede yapılan güncellemelerde çalışmaların şeffaf olması gerektiği vurgulanmıştır. Ayrıca önemli bir madde olarak Beyaz Saray'a bağlı olacak bir siber güvenlik Ofisi kurulması ve ulusal güvenlik konseyine üye olacak şekilde bir "Siber Çar"ın bu ofisin başında yer alması kararı alınmıştır ve uygulanmıştır. Daha önceki çalışmalarda da belirtilen, kurumların sorumluluklarının belirlenmesi ve böylelikle yetkinin belirsiz olması sorununun ortadan kaldırılması hedefi, bu zamana kadar hala sağlanamamıştır. CNCI direktifinin en son halinde de bu hedef belirtilmiş ve hükümet kuruluşlarının ortak sorumluluklarının olmaması gerektiği, ayrıca her kurumun görev ve yetkilerinin kesin olarak belli olması gerektiği vurgulanmuştır.

Bu güncellemede sunulan organizasyon şeması aşağıda yer almaktadır. Bu organizasyon şeması tam olarak uygulanmamış olsa da Beyaz Saray'da direkt başkana bağlı olarak çalışan siber çar atanması planı gerçekleşmiştir.



Şekil 1: ABD'de siber güvenlik uygulamaları organizasyon şeması[6]

Bu organizasyona göre; siber güvenlikle ilgili çalışmalar yapan ve çeşitli yetkileri olan tüm kurumlar, Siber Çar'a bağlıdır. Siber Çar da başkana bağlıdır. Siber güvenlik sisteminin bu şekilde çalışması, hem olaylara hızlı müdahale edilmesini hem de koordinasyonun kolay yapılmasını sağlaması açısından başarılı bir yöntem olarak görülmektedir. Siber Çar'a bağlı olan kurumlardan DSH, siber savunmadaki en önemli görevi yürüten CERT organizasyonunu barındırmaktadır. Ayrıca ulusal siber tepki koordinasyon grubu da DSH altında faaliyet yürütmektedir. Koordinasyon grubunun amacı, ulusal çapta bir siber saldırı olması durumunda kurumların çalışmalarını koordine ederek, karışıklıkları önlemek olarak belirtilmektedir. Bununla birlikte, CIA (Central Intelligence Agency), NSA (National Security Agency) ve Savunma Departmanı (Departman of Defense) kurumları da siber güvenlik alanında çalışmalar yürütmektedir. Organizasyon şemasından da anlaşılacağı gibi, ABD'de orduya ait siber güvenlikten sorumlu kurumlar da Siber Çar'a bağlıdırlar.

NSA, ABD'nin siber güvenlik konusundaki en önemli birimidir. Geçmişten bu yana sinyal ve bilgi istihbaratı konusunda çalışmalar yapan bu kurum, günümüzde de internet ağlarının takibini yapmaktadır. Yaptığı çalışmalarla her türlü bilgiye erişebildiği düşünülen kurumun bu çalışmaları, ulusal güvenlik ile kişisel bilgilerin gizliliği arasındaki dengenin sağlanması noktasında tartışma

[6]Orjinal çizim için bknz.İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü."Siber Güvenlik Raporu" (2012, Mayıs)

konusudur. NSA'nın takip ettiği ağlarda meydana gelecek bir saldırı durumunda müdahale etmekle görevli birim, USCYBERCOM (US Cyber Command)'dur. Siber komandolar olarak da adlandırılan Uscybercom, savunma bakanlığı bilgi ağlarının operasyon ve savunmasını yönetmek, gerektiğinde askeri siber uzay harekatlarını icra etmek, ABD ve müttefiklerine siber uzay serbestisi sağlamak ve hasımlarına engel olmak amaçlı eylemler planlar, koordine eder, birleştirir, senkronize ve ica eder.[7] Uscybercom, 5 amaca odaklanmaktadır:

- Siber uzaya da kara hava ve deniz gibi bir harekat alanı olarak muamele etmek,
- Burada başarılı olmak için yeni güvenlik konseptleri uygulamak,
- Diğer kurumlar ve özel sektör ile ortaklık geliştirmek
- Uluslararası ortaklar ile ilişkiler geliştirmek
- Bu uzayda ordunun nasıl savaşacağına ve kazanacağına yönelik yenilikleri teşvik etmek için yeni yetenek geliştirmek

NSA ve Uscybercom, biribiri ile koordine şekilde çalışan iki kurumdur ve bu iki kurumun başında aynı komutan yer alır. ABD, siber güvenliğe sadece bakanlıklar nezdinde yönetilen ve devlet kurumlarının korunmasını sağlayan bir oluşum olarak bakmamaktadır. Gelinen noktada siber güvenlik alanının bir savunma ve saldırı alanı olarak geliştirilmesi için çalışmalar yürütmektedir. Pentagon'un 2013 bütçe planında 53 kere "siber" den bahsedilmiştir. 2014 yılındaki bütçe planında ise diğer ABD askeri bütçelerinin kesintiye uğramasına rağmen, CYBERCOM kurumunun harcamaları ikiye katlanmış ve "siber" kelimesi 147 kere geçmiştir.[8] Ayrıca ABD, ordunun siber yapılanması için Silikon Vadisi ile de işbirliği yapmıştır.[9]

CIA/NSA'nın alt birimleri olan IC-IRC (Intelligence Community-Incident Response Center) ve NTOC (Threat Operations Center) ile Birleşik İş Gücü (Joint Task Force) ve Global Ağ Operasyonları (Global Network Operations) birimleri siber savunmada önemli görevler üstlenmektedir.

[7]Singer, P. W., Friedman, Allan. "Siber Güvenlik ve Siber Savaş" (Çev. Ali Atav). Ankara, 2015

[8]Singer, P. W., Friedman, Allan. "Siber Güvenlik ve Siber Savaş" (Çev. Ali Atav). Ankara, 2015

[9]"Sardıç: ABD Siber Ordu için Silikon Vadisi ile Çalışıyor" (2015, 14 Eylül). Erişim tarihi: 02.01.20.16.

Tüm bu kurumların çalışmalarında kullandığı en önemli yazılımlar: EINSTEIN, TIC yazılımları ve içeriği hakkında çok fazla bilgi verilmeyen Clasified Programs diye adlandırılan programlardır.

- EINSTEIN: EINSTEIN programı, US-CERT tarafından geliştirilmiş, ABD kurumlarına ait ağ trafiğini izlemeyi amaçlayan yazılımdır. 2003 yılında çıkan ilk sürümü sadece giriş ve çıkışları kaydederek, takip edilmesine imkân sağlarken, 2008 yılında çıkarılan 2. sürümü ile saldırıları tespit edip uyarı oluşturma özelliğine kavuşmuştur. Bir günde 30000 uyarı oluşturan EINSTAIN 2, herhangi bir müdahalede bulunmamakta, müdahaleyi DSH siber güvenlik personelleri yapmaktadır. Programın 2010 yılında çıkan son sürümü, EINSTAIN Accelerated (E3A) olarak adlandırılmaktadır. Bu son sürüm, tespit ettiği atakları sınıflandırma ve gerektiğinde engelleme (blocked) ayrıca potansiyel tehditleri de tespit etme özelliğine sahiptir. Ek olarak tüm devlet kurumlarına ait ağları bir araya toplayarak DSH personellerinin kolayca müdahale etmesini sağlamaktadır. DHS, bir sonraki sürüm için özel sektör ile birlikte çalışıp, yeni teknolojileri incelemektedir. EINSTEIN programı, Eylül 2015 itibari ile 17 devlet kurumunu korumak için kullanılmaktadır ve koruma başarısı %45 civarındadır.[10]
- TIC: Programın uzun ismi, Trusted Internet Connections'dır. Bu sistem, devlet kurumları içinde kullanılan bağlantıların sayısını önemli ölçüde düşürerek daha güvenli ve kontrol edilmesi kolay bir sistem oluşturulmasını sağlayan, DHS tarafından geliştirilmiş yazılım ve donanım bütünüdür. TIC ve EINSTEIN, devlet kurumlarını korumak için birlikte çalışmaktadır.

- Clasified Programs (Gizli Programlar): ABD, siber güvenlik alanında geliştirdiği birçok programa sahiptir. Bu programlar hakkında çok fazla bilgi bulunmamaktadır. Bu yazılımlara, güvenlik amacıyla Facebook, Gmail, Microsoft, Yahoo, Apple, Google, Skype gibi uygulamalardan veri toplayan PRISM programı örnek verilebilir.[11]

ABD, siber güvenlik organizasyonunda adaletten sorumlu olan çalışma alanı, Hukuk Departmanı (DOJ) altındaki Bilgisayar Suçları ve Fikri Mülkiyet Birimi'dir. Bu birim de siber güvenlikle ilgili sorumluluklara sahiptir. DOJ altında

[10]http://www.dhs.gov/einstein
[11]Detaylı bilgi için bknz. https://nsa.gov1.info/surveillance/

yer alan kurumlardan biri olan FBI tarafından, 2001 yılında internet suçları şikayet merkezi (Internet Crime Complaint Center/IC3) kurulmuştur. Bu merkez, internet suçlarının raporlanmasını ve meydana gelmeden engellenmesini amaçlamıştır. Bu amaçta birçok olay tespit edilmiş ve engellenmiş olmasına rağmen, tespit edilen olay sayısı toplam olayların çok az bir kısmını oluşturmaktadır.

Her ülkede olduğu gibi ABD'de de siber güvenlik uzmanlarının bulunması ile eğitilmesi önemli ve özel çaba harcanan kalemlerdir. ABD'de siber güvenlik konusunda eğitim veren kurumlardan biri, DSH'dır. DSH altında siber güvenlik stajyerlik programı (Cybersecurity Internship) adındaki oluşum, siber güvenlik uzmanlarını stajyerlik seviyesinden eğitmeye başlayan, eğitimlerde uzmanlarla birebir çalışma, gerçek olaylar üzerinden öğrenme, kullanılan araçları (tool) öğrenmek şekilde eğitimlerin bulunduğu bir programdır. Bu programın devamında yer alan Secretary's Honour programı ise lisans ve yüksek lisans düzeyinde siber güvenlik uzmanları yetiştirmeyi hedefleyen bir programdır. ABD'deki siber güvenlik eğitimi veren bazı kurumlar şunlardır:

- Ulusal Kriptoloji Okulu: Bu okul, NSA'nın uzmanlarının büyük bölümünü oluşturan ve ne şekilde eğitim verdiği konusunda fazla bilgi bulunmayan gizli bir okuldur. 1960'lı yıllarda zamanın teknolojisine göre ulusal kriptologlar, yetiştirmek için kurulan okulun müfredatını zamana göre sürekli güncelleyen bir okuldur. Öyle ki "2006 yılında "siber" kelimesinin hiç anılmadığı bu okulda, bugün siber güvenlik dersleri, sadece bu alan için açılmış yeni bir enstitüde verilmektedir."[12] Okul, Dakota Devlet Üniversitesi işbirliğ yapmıştır. Söz konusu işbirliği ile liseden sonra askere katılan öğrencilerin üniversite okuyarak siber güvenlik konusunda uzmanlaşmalarına imkan verilmiştir. Ayrıca okul, siber güvenlik uzmanlarının en önemli özelliği olarak gördüğü dil eğitimine de önem vermektedir ve bu amaçla Arapça, Çince, Hintçe, Farsça, Portekizce, Rusça, Swahilice, Türkçe, Urduca, Korece gibi dillerin öğrebilmesi için çeşitli üniversitelerle çalışmalar yürütmektedir. Okulun dikkate değer bir diğer özelliği de çocukların teknoloji

[12] http://siberbulten.com/uluslararasi-iliskiler/abd/amerikanin-kriptologlarini-yetistiren-gizli-okulun-hikayesi/?utm_content=buffer40b2d&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer

konusundaki farkındalık ve yeteneklerini artırmak için yaz kampları düzenlemesidir. Bu kamplar, bilinen kamplardan farklı olarak siber güvenlik hatta hackerlık dersleri vermektedir.

- NICCS: Siber güvenliğe ilgisi olan herkesin başvurabildiği bir eğitim kurumudur.
- NICE: Devlet kurumları ile özel sektörün ortaklığında eğitim vermeyi, değişim yapmayı hedefleyen kurumdur. İlkokul ve ortaokul seiyesinde siber güvenlik eğitimleri vermektedir. NICE'ın amacı, oluşabilecek tehditlerin ve hızla gelişen teknolojinin önüne geçecek kişileri yetiştirmek olarak belirtilmektedir.

ABD'de siber güvenlikle ilgili çalışacak uzmanların yetiştirilmesi ve seçilmesinden sorumlu kurumlar da bulunmaktadır. Bunların başında yıllardır siber suçlarla mücadele eden FBI Kurumu gelmektedir. FBI, devlet kurumlarına uzman yetiştirmek ve polislere bilgisayar suçlarının soruşturulmasında yardım etmek gibi faaliyetler yürütmektedir. Ayrıca ABD'nin eleman alımında kullandığı National Cyber Security Workforce Framework adındaki sistem, devlet kurumlarına siber güvenlik elemanı alımı için kullanılmaktadır.

FBI'ın bağlı oldu DOJ ise avukatlara siber suçların anlaşılması, soruşturulması sırasında yapılaması gerekenlerin bilinmesi ve doğru şekilde ilerlenmesi için eğitimler vermektedir.

II. Hindistan ve Siber Güvenlik Uygulamaları

Hindistan, sahip olduğu nüfus yoğunluğu ve bilişim sektörünün gelişmiş olmasından kaynaklı olarak internet kullanımı konusunda listenin başlarında yer alan ülkelerden biridir. Bu nedenle ülke yönetimi de siber güvenlik konusuna büyük bir önem vermektedir. 2010 yılından bu yana akademik ve devlet düzeyindeki çalışmalarla siber güvenlik konusunda adımlar atılmış, diğer ülkeler incelenerek hedefler koyulmuş ve yeni atılımlar yapılmıştır.

Hindistan'da Savunma Bakanlığı bünyesinde de siber güvenlikten sorumlu birimler bulunmaktadır ancak ülkede siber güvenlik konusunda en yetkili kurum, ABD'deki NSA kurumuna benzer bir yapı olan Ulusal Güvenlik Kurumu (NSC) dur. Bu kurum ile ortak çalışmalar yürüten ve tehditlere karşı savaşmayı hedefleyen ISTF (Information Security Task Force) kuruluşu da en üst düzeyde yetkiye sahiptir. ISTF'nin yaptığı çalışmalar ile 2013 yılında ulusal siber güvenlik

planı belirlenmiştir. Bu planın öne çıkan önerileri, ülke çapında siber güvenlik alanından çalışan veya sorumluluğu olan kurumların rollerinin açık bir şekilde belirlenmesi; siber güvenlik alanında çalışmayı teşvik etmek amaçlı, vergi indirimi sağlanması; siber saldırılarda, kurumlar arası bilgi paylaşımının sağlanması; kurumların kontrol edilmesi ve sertifikalandırılması konusunda düzgün bir yapı oluşturulması (ISO 27001 ISMS sertifikası, Penetratsyon testleri, uygulama güvenlik tetsleri, web güvenlik testleri, vb.); siber güvenlik konusunda farkındalık oluşturmak; devlet kurumlarında ve özel sektörde siber bilişim konusunda eğitimler verilmesini teşvik etmek; siber güvenlik eğitimleri için kamu – özel sektör ortaklığı sağlamak; siber güvenlik labaratuvarları açmak şeklindedir. Bu maddeler çerçevesine yapılan çalışmalarla siber güvenlik konusunda önemli adımlar atılmıştır. Devlete ait önemli ağların ve kritik altyapıların korunmasını sağlamak amacıyla, Bilgi güvenliği politikası oluşturulmuştur. Vatandaşları bilgilendirmek amacıyla bilgi güvenliği konusunda kampanyalar yürütülmüştür.

Hindistan'ın siber güvenlikle ilgili çalışmalarda en çok göz önünde bulundurduğu noktalardan biri, siber bir saldırı durumunda devlet kurumlarının müdahalesinin sağlanabilmesi; bu yeteneğin çalışanlara kazandırılması olmuştur. Bu amaçla, çalışmalarını plan hazırlamak, kampanya yürütmek gibi pasif sayılabilecek adımların yanında teknik boyutta çalışmalara ağırlık vererek sürdürmüştür. Teknik çalışmalardan en önemlisi, siber güvenlik laboratuvarı oluşturma hedefini gerçekleştirmiş olmasıdır. Bu laboratuvarda, sistemlerin korunması, erken uyarı sisteminin oluşturulması, ağların 7/24 takibinin sağlanması, devlet kurumlarının yanında özel sektörde yer alan büyük ve küçük firmaların da siber güvenliğinin sağlanması, siber saldırılar ve siber terörizme karşı kriz yöntemi planı oluşturulması gibi konularda çalışmalar yapılmaktadır.

Ülkede ihtiyaç durumunda yararlanılmak üzere ulusal güvenlik veritabanı (NSD) oluşturulmuştur ve bu veri tabanında siber güvenlik uzmanlarının bilgileri tutulmaktadır. Bu veritabanı sayesinde siber güvenlik uzmanlarının çalışma alanları, daha önceki çalışmaları, yaşadığı yer ve bu tarz bilgilerine hızlıca ulaşılması, böylece meydana gelen bir olayda devlet kurularının teknolojik ve lojistik açıdan güç sahibi olması ve mümkün olan en hızlı şekilde müdahale edilmesi amaçlanmaktadır. Siber güvenlik araştırmaları yapan bir kuruluş olan Ulusal Siber Savunma Araştırma Merkezi, siber suçlarla mücadele için el kitabı dağıtma, çeşitli eğitimler verme gibi aktivitelerde bulunmaktadır.

Hindistan'da birçok siber güvenlik araştırma ve eğitim merkezi mevcuttur. Örneğin; CERC diye bilinen Cyber Security Education and Research Centre, öğretmenler için farkındalık semineri de verilen siber güvenlik konusunda programlama dersleri ve danışmanlığı da verilen çok yönlü bir eğitim kuruluşu imajı çizmektedir. CERC'de siber güvenlik konusunda temel eğitimler (base) ve daha ileri seviyede eğitimler (training) olmak üzere 2 seviyeli bir eğitim verilmektedir. Eğitim verilen alanlara, siber güvenlik hukuku, siber güvenlik, dijital kanıtlar, e-keşif eğitimleri örnek verilebilir. Kurumda teknik eğitimlerin yanında, toplumun farkındalığını artıracak eğitimler ve seminerler de verilmektedir. CERC kurumu altında siber güvenlik eğitimi veren, Centre of Excellence for Cyber Security Research and Development in India (CECSRDI) kurumu yer almaktadır. Bu kurumun amacı, siber güvenlik konusunda farkındalık yaratmak, Hindistan için siber güvenlik yazılımları geliştirilmesi için ve Hindistan'ın siber suçlarla mücadele konusunda geliştirilmesi için çalışmak olarak belirtilmektedir.

Birçok ülke gibi Hindistan da siber güvenlik konusunda aldığı aksiyonları askeri düzeyde de uygulamaktadır. Bu konuda en iyi durumdaki iki ülke olan ABD ve İsrail, Hindistan'ın rol modeli olmuştur. Bir ülkenin savunması, gelişen teknolojinin de etkisiyle kullanılan araçların yazılım alt yapısına sahip olması nedeniyle, siber düşmanlar açısından saldırılması en mantıklı olan departman iken; devletlerin de en çok yatırım yapması ve üzerinde düşünmesi gereken departmandır. Hindistan bu amaçla, 2002 yılında askeri yapılanma içerisindeki Hindistan istihbarat teşkilatı (DIA) ve Ulusal Teknik İstihbarat İletişim Merkezi, siber birlik olarak görevlendirilmiş ve siber güvenlikle ilgili tehditleri tespit edip devlet kurumlarını uyarma, gerekirse karşılık verme görevini üstlenmişlerdir.Hindistan, siber güvenlikle ilgili yatırımlarından birini de askeri alanda gerçekleştirmiş ve elektronik savaş sistemlerinin test edilmesi için 2 adet tesis oluşturmuştur. Ayrıca ülkenin ikinci siber güvenlik laboratuvarı, Askeri Telekomünikasyon Mühendisliği Üniversitesi dahilinde kurulmuştur. Bu laboratuvar, ordunun siber güvenlik departmanı çalışanlarına askeri ağların güvenliği için sinyal ve veri iletim ağlarının takibi ile ilgili eğitimler vermeyi amaçlamaktadır. 2012 yılında açılan laboratuarın 2017 yılında tam olarak ağ merkezi kuvveti olarak hizmet vermesi planlanmaktadır. Bu laboratuvar, çalışanları her türlü siber saldırıya karşı tam olarak donatmayı hedeflemektedir.

Hindistan devleti tarafından uygulanan önemli ve örnek alınabilecek adımlardan biri de önemli belgelerin korunması için güvenlik standartı geliştirmiş olmalarıdır. Bu çalışma, teknoloji çağında, yazışmaların başka bir ülke tarafından geliştirilmiş programlar aracılığı ile saklanmasının akıl dışılığı düşünüldüğünde önemli bir adım olarak nitelendirilebilir. Bu gibi bilgi ve belgelerin saklanması iletilmesi konusunda hem ağ güvenliği politikaları ve standartlar hem de bu bilgilerin saklandığı kurumlarda çalışan perdonelin eğitimleri önem kazanmaktadır.

Siber güvenlik konusunda birçok çalışma yapan Hindistan, 2005 yılında ulusal CERT kurumunu kurmuştur. CERT-In adındaki bu kurum, siber güvenlik konusunda çalışmalar yapan birçok ülkede bulunan ve bilgisayar sistemlerini korumak, gözetlemek, saldırıları tespit etmek ve zamanında müdahalede bulunmak amacıyla çalışan CERT kurumlarındandır. CERT-In kurumu, 7/24 hizmet saldırı ihbarlarına karşı destek hizmeti vermek, siber saldırıların tespiti ve uyarı verilmesi için takipte olmak, saldırılara karşı kamu ve özel sektör kurumlarına tavsiyelerde bulunmak gibi sorumluluklara sahiptir. Ayrıca diğer ülkelerdeki CERT kurumları ile iritbat halinde olan, bu sayede hem gerektiğinde bilgi alışverişi sağlayabilen hem de yeni virüsler, saldırı teknikleri, savunma biçimleri gibi konulardan haberdar olma imkanına sahip bir kurumdur.

CERT-In, hem devlet kurumları hem de özel sektördeki kurumlar ile irtibat halinde bulunan bu açıdan hem iletişim hem de koordinasyonu sağlayan aracı kurum konumundadır. Siber güvenik konusunda büyük ilerleme kaydetmiş özel firmalarla ve Hindistan dışındaki siber güvenlik alanında çalışan firmalarla iletişim halinde olup bu firmalar ile işbirliği içerisindedir. CERT-In, kurumların bilgilendirilmesi ve siber güvenlik açısından test edilmesi, takip edilmesi konularda da çalışmalar sürdürmektedir. 2010 yılında yaptığı bir çalışma olan "Siber Saldırılar ve Siber Terörizme Karşı Kriz Yönetimi Planı", devlet kurumları tarafından uygulanması gereken adımları içermektedir. Hindistan'da CERT-In tarafından yürütülen bir diğer önemli çalışma da kritik öneme sahip alanlarda çalışan kamu ve özel kuruluşlarda standartlara uygun dönüşümün sağlanmasını teşvik etmek ve danışmanlık vermektir. Özellikle bankacılık, bilgi sistemleri, telekomünikasyon gibi stratejik öneme sahip alanlarda hizmet veren kurumların ISO 27001 standardına uygun hale getirilmesi için çalışmalar sürdürülmektedir.

Ayrıca bu gibi kurumların penetrasyon testleri de yine CERT-In önderliğinde yapılmaktadır.

III. İsrail ve Siber Güvenlik Uygulamaları

Siber güvenlik alanında yapılan araştırmalarda, her ülkenin siber güvenlik staratejisi oluşturmak için yaptığı ön hazırlıklarda hatta akademik makale ve çalışmalarda bile siber güvenlik konusunda geldiği yer ve yaptığı çalışmalardan dolayı sıklıkla adı geçen, başarısının incelendiği makalelerin bulunduğu bir ülkedir İsrail.Ortadoğu'da siber güvenlikteki atılımları ile diğer ülkelerin çok ilerisindedir.2015 yılında yapılan bir araştırmaya göre ABD'den sonra siber güvenlik alanındaki en güçlü 2.ülke, İsrail'dir. İsrail'in 8 milyonluk nüfusu ve küçük sayılabilecek yüz ölçümüne rağmen siber güvenlikte bu derece ilerlemesinin sebebi olarak, etrafındaki tüm ülkeler ile olan siyasi çekişmesi ve bu nedenle sadece fiziksel anlamda bir savunmanın yeterli olmayacağının bilincine vararak, teknolojik alanda da savuma stratejisi geliştirmesi gösterilmektedir. Bu konuda yapılan bir araştırmada İsrail'in siber güvenlikteki başarısının temelinde üç uygulamanın olduğundan bahsedilmektedir. Bu üç uygulama: siber ordu kurulması, ulusal savunma kurumları ile özel sektör işbirliğinin kurulması ve siber güvenlik alanındaki girişimcilerin desteklenmesidir.[13]

İsrail savunma bakanlığı (IDF), siber savaş için iki adet "elit birim" kurmuştur. Unit 8200 (Birim 8200) ve C4I adındaki bu kurumları, çalışmalarını "Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnasisance" diye açılımı olan C4ISR denen bir sisteme dayandırmaktadır. Bu formülden de anlaşılmaktadır ki İsrail siber güvenlik konusunda yapılan çalışmaları, bir muharebede yapılan bir savunma için kaçınılmaz olarak görmektedir. Unit 8200, sinyal toplamak ve kod çözmekten sorumlu askeri birimdir. Altında Hatzav birimi gibi birçok küçük siber güvenlik birimi barındırmaktadır. Yazılım konusunda uzman kişileri işe aldığı gibi lise ve üniversite seviyesindeki gençleri de eğitmek, yani gelecek nesilin siber güvenlik uzmanlarını yetiştirmek için almaktadır. Siber güvenlik konusunda tüm ülkelerin en önemli sorunu olan eğitimli personel ihtiyacını karşılamak için çalışmalar yürütmekte, adeta siber güvenlik okulu gibi çalışmaktadır. İsrail devleti, dışarıdan

[13]Chaturvedi, M. M., Gupta, MP, Bhattacharya, Jaijit. "Cyber Security Infrastructure in India: A Study". Erişim tarihi: 11.12.2015. http://www.iceg.net/2008/books/2/9_70-84.pdf

yazılım almak, araştırma ve geliştirme çalışmaları için başka ülkelere güvenmek yerine kendi eğittiği uzmanlar ile çalışmayı tercih etmektedir. Bu birimin mezunları, sadece devlet kurumlarında değil, özel şirketler de çalışmakta, bu vesile ile devlet kurumu-özel sektör bağlılığı da oluşturulmuş olmaktadır. Zaten şu an ülkede önemli işler yapan siber güvenlik şirketlerinin büyük kısmını kuran kişilerin Unit 8200 mezunu olduğu belirtilmektedir. Burada önemli bir nokta, Unit 8200'ün başvuru almak yerine gençleri "keşfetmeyi" tercih etmesidir. 16-18 yaş arasıdaki hem erkek hem de kız öğrencilerin eğitildiği kurumda, erkekler askeri eğitim de aldıkları için 3 yıl; kızlarsa 2 yıl süren yazılım ve hackerlık dersleri almaktadır. Verilen eğitimlerde, eğitimlerin teorikten pratiğe geçebilmesi için simülatör ile çalışılmakta, bu sayede öğrenciler bir siber saldırı anında alması gereken aksiyonlar vee alacakları tedbirler konusunda pratik yapabilmektedir.Bu okulun eğitim seviyesi Harward, Yale gibi üniversitelere denk olarak gösterilmektedir.[14]

Bu iki birim Negev Çölü'nde üstün teknoloji ile donatılmış bir kampüste çalışma yapmaktadır. Unit 8200, tüm dünyadan sinyal bilgisi toplamak ve kod çözmekten sorumluyken, C4I'nın amacı askeri şebeke ve ağları siber saldırılarıa karşı korumaktır. Unit 8200, ABD'nin NSA yapılanmasına benzetilebilir ve İsrail savunmasının en büyük birimidir. Altında birçok başka brim bulunduran Unit 8200, siber güvenlik konusunda çok iyi bir durumdadır. Öyle ki; 2010 yılında Hindistan ve ABD de dahil birçok ülkedeki 130000 bilgisayara bulaşan[15]; ancak bulaştığı bilgisayarların %60'ının İran'da[16] bulunması nedeniyle İran'ın nükleer tesisinde yer alan bilgisayarları hedef aldığı düşünülen Stuxnet virüsünü, Unit 8200'ün ürettiği, her ne kadar kanıtlanamasa da, sıklıkta söylenegelen bir durumdur. Stuxnet virüsünün sistemlere bulaştırılmasınıdaki iki önemli nokta, virüsün internete ihtiyaç duymadan bulaşmış olması ve SCADA sistemlerini hedef alması olmuştur.

Unit 8200 ve C4I kurumları, sürekli koordinasyon halinde çalışmaktadır. Bu kurumların hepsi, tıpkı ABD'de olduğu gibi, çalışmalarını düzenleyen,

[14] Reed, John. "Unit 8200: Israel's cyber spy agency" (2015, 10 Temmuz). Erişim tarihi: 18.11.2015. http://www.ft.com/cms/s/2/69f150da-25b8-11e5-bd83-71cb60e8f08c.html

[15]Bakır, Emre. "5. Boyutta Sacaş: Siber Savaşlar – I" (2012, 20 Aralık). Erişim tarihi:21.12.2015. https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-i.html

[16]Singer, P. W., Friedman, Allan. "Siber Güvenlik ve Siber Savaş" (Çev. Ali Atav). Ankara, 2015

iletişimlerini sağlayan bir "siber şef"e bağlıdır. Unit 8200 altında yer alan birimlerden biri olan Hatzav Birimi, açık kaynak istihbaratı toplamaktan sorumludur. IDF altında bulunan en büyük teknoloji birimi olan Lotem Unit (Lotem Birimi) C4I yapısının altında yer almaktadır. Lotem Birimi, telekomünikasyon ve bilgi teknolojilerinin güvenliği üzerine çalışmalar yürütmektedir. Ayrıca IDF'nin bulut bilişim çağına adaptasyonundan sorunlu birim de Lotem'dir.

2015 yılında IDF'nin aldığı kararla siber komandolar yetiştirmeye ve bu komandoları önemli ve riskli sistemlerdeki operasyonlarda kullanma kararı alınmıştır. Bu kapsamda, başlangıç için siber komandol birliği IDF altındaki C4I ve Askeri İstihbarat birimi (DMI) içinde yer alacak, sonrasındaysa IDF'nin siber alandaki ekiplerinin yeniden yapılandırılması planlamaktadır. İsrail'de siber aktivitelerin, askeri operasyonlarda saldırı ve savunma amaçlı kullanımı gittikçe artmaktadır. Bu güne kadar C41 ve DMI altında yer alan Unit 8200 birimlerinin sorumluluğu altındayken bu iki ekibin değişen koşullara hızlı uyum sağlamak konusunda geride kaldığı düşünülmektedir. Ayrıca DMI'nın sorumluluğunu çok olması nedeniyle siber güvenlik alanında yeterli etkinliği gösteremediği düşünülmekte bu nedenle de sadece siber güvenlik ile ilgilenecek siber komandolar biriminin oluşturulması 2016 yılı çalışmalarında yer almaktadır. Planlanan siber komanda timinin en göze çarpan özelliği, direkt olarak, Chief of the General Staff olarak bilinen IDF yöneticisine bağlı olmasının planlamasıdır.

İsrail'de IDF dışında siber güvenlik çalışması yapan birçok kamu kurumu ve sivil kuruluş da mevcuttur. National Cyber Bureau, The Institute for National Security Studies ve Cyber Authority, bu alanda çalışan sivil kurumlardır. Bunun yanı sıra, GSS ve Mossad da siber güvenlik konusunda çalışmalar yapmaktadır. Bu kurumların hepsi birbiri ile birlikte çalışmaktadır.

İsrail, hassas bilgisayar sistemlerinin ve hassas verilerin korunmasının önemini ilk fark eden ülkelerden biridir. Siber güvenlik ile ilgili ilk çalışmaları 1996 yılının başlarına tekabül eder. 1996 yılında, hükümet siber saldırılara karşı yapılacakların belirlenmesi için çalışmalar yürütmüş ve bu çalışmaların sonucunda 1997 yılında devlete ait ağların korunması ve güvenli internet kullanımını sağlamak amacıyla Tehila Projesi başlatılmıştır.

Değişen teknoloji ile "savaşmak" terimi de geçmişteki anlamından farklı bir anlama evrilmiştir. Günümüzde topla füzeyele savaşmaktan daha etkili yöntem

varsa o da teknolojiyi kullanarak savaşmaktır. İsrail de bunu fark ederek atılımlar yapmış bir ülkedir. Bir toplumda insanların, yokluğunda en çok etkileneceği yapıların korunması çok daha önemlidir. Örneğin bir şehrin su sistemine, elektik sistemine yapılacak bir saldırı, hele bir de saldırı altındaki ülkenin bu konuda savunma yapacak gücü yoksa, çok daha yıkıcı olabilir. Bu nedenle İsrail devleti, su, elektrik, doğal gaz gibi sistemleri siber tehditlerden korumak adına SCADA[17] sistemleri ile sürekli denetlemektedir. SCADA sisteminin amacı büyük bir alanda çalışan bir sistemi veya tesisi kontrol altında tutmak, denetlemek ve yönetmektir. Sistemi izleme, kontrol etme, veri toplama ve log oluşturma işlevlerini yerine getiren insan-makina veya makine-makine arayüzü ile çalışan sistemlerdir. Bu sistemler, tesislerin siber saldırıya uğraması ihtimaline karşı ikaz sistemlerinin olması hasebiyle kullanılması elzem bir sistemdir.

İsrail devleti, siber güvenlikte çeşitli atılımlar yaptığı gibi uluslararası işbirlikleri yapmak için de çalışmalar yürütmektedir. Bu konuda en büyük partneri ABD olsa da diğer ülkelerle de işbirliği içerisindedir. 2013 yılında İtalya ile imzalanan deklarasyonla iki ülke, siber uzay konusunda işbirliği yapmıştır. Bu deklarasyon İsrail'in ilk anlaşması olsa da son olmayacaktır. 2014 Mayıs ayında Japonya ile anlaşma yapılmış, 2014 yılının şubat ayında İsrail AeroSpaces Industries (IAI), Singapur'da Siber Erken Uyarı Sistemleri Araştırma ve Geliştirme merkezi kurulması kararını imzalamıştır. Bu merkezin, siber erken uyarı sistemleri prototipi üretip, bu ürünleri Singapur ve dışında pazarlaması planlanmaktadır. Bu merkezdeki araştırmaların kritik ve acil alanlar olan, siber saldırganların gerçek zamanlı olarak tespit edilmesi, siber geo-location[18] çözümleri ile siber saldırganların fiziksel lokasyonunun belirlenmesi, ileri düzey anomali tespit sistemleri, gibi projeler üzerine yoğunlaşması beklenmektedir.

İsrail, siber güvenlik konusunda yurt içinde ve dışında dinamik işbirlikleri oluşturmak, eğitim-askeriye-endüstri dünyalarının birlikte çalıştığı simbiyotik bir siber uzay oluşturmayı hedeflemektedir. Bu nedenle 27 Ocak 2014'de ülkenin kuzeyinde yer alan Beer-Sheva'da ulusal Siber Merkez (CyberSpark)'in kuruluşunu duyurmuştur. Bu merkezin amacı Unit 8200 ve Lotem Birimi gibi askeri siber birlikleri, IBM ve Deutsche Telekom gibi yüksek teknoloij sahibi

[17]Supervisory, Control ve Data Acquisition kelimelerinin baş harflerinin bir araya gelmesiyle oluşturulmuştur.Geniş alana yayılmış tesislerin tek bir merkezden izlenebildiği sistemlerdir.
[18] İnternet tarayıcının kendi içindeki komutların kullanılmasıyla, kullanıcının yerinin saptanması işlemidir.

araştırma ve geliştirme şirketlerini ve siber güvenlik alanında çalışma yapan akademik kadrolar ile sivil kuruluşları bir araya getirmektir. Bu çalışmanın 9 milyon dolara mal olacağı tahmin edilmektedir.[19]

İsrail, genel olarak siber güvenlik alanında sürekli atılımlar yapan aktif bir yaklaşım sergilemektedir.

IV. Çin ve Siber Güvenlik Uygulamaları

Çin de siber güvenliği sadece gelişen teknojinin getirdiği dezavantajları egale etmenin gereği olarak değil, aynı zamanda modern dünyanın savaş aletlerinden biri olarak gören ülkelerden biridir. Çin başkanı Xi Jinping, "Siber güvenlik olmadan, ulusal güvenlik olamaz." diyerek siber güvenliğe bakış açılarını özetlemiştir.[20] Bu nedenle siber güvenlik alanında çalışma yürütüne en önemli ekipler askeri ordunun içerisindedir. Ordunun siber güvenlik alanındaki çalışamaları 90'lardan beri sürmektedir. Çin Ordusunda siber güvenlik alanında çalışan, ülkenin bilişim altyapısını koruyan iki adet ekip bulunmaktadır. Bu ekipler, savunma ve önlem amaçlı, ülkedeki tüm internet trafiğini izlemektedir. Bu ekiplerde çalışan toplam personel sayısının 130000 civarında olduğu belirtilmektedir.[21] Ordudaki ekiplere ek olarak ülkede siber güvenlik alanında araştırma ve geliştirme faaliyetleri sürdüren siber güvenlik enstitüleri bulunmaktadır. Ordu (PLA) sahip olduğu tüm teknik ekipmanlar ile AR-GE çalışması yapan enstitülere destek vermektedir. Bu enstitüler de diğer ülkelerin sistemlerine ait şifreleri kırmak amaçlı yazılımlar geliştirilmektedir. Çin ordusunda da İsrail ordusunda olduğu gibi siber güvenlik alanından eğitimler verilmekte ve siber güvenlik uzmanları yetiştirilmektedir. 2014 yılında PLA altında görev yapmak üzere Siber Uzay Stratejik İstihbarat Araştırma Merkezi (Cyberspace Strategic Intelligence Research Center) kurulmuştur.Bu merkezin amacı ülkenin ulusal bilgi güvenliğini sağlamak ve bu yönde araştırma ve geliştirmeler yapmaktır. Bunun yanı sıra; ülkede internet istihbaratı için

---

[19]Singer, P. W., Friedman, Allan. "Siber Güvenlik ve Siber Savaş" (Çev. Ali Atav). Ankara, 2015

[20] Orijinal çizim için bknz. China Monitor. "Cyber Security in China: New Political Leadership Focuses on Boosting National Security" (2014, Aralık). Erişim Tarihi: 05.12.2015 http://www.merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf

[21]İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü. "Siber Güvenlik Raporu" (2012, Mayıs).Erişim tarihi: 10.11.2015

araştırmalar yapmak konusundan yetkili bir kurum olması, etkili ve dinamik bir siber uzay oluşturmak, hassas sistemler için üst düzey koruma sağlamak amaçlarına hizmet etmekte ve akademik kadrolar ile de işbirliği yapmaktadır. Çin, PLA altında çalışma yürüten Mavi Ordu isiminde 30 kişilik Çin'in en yetenekli beyinlerinden oluşan bir orduya sahiptir. Bu Ordu'nun PLA'nın intermet ağlarını saldırılardan korumakla görevli olduğu belirtilmiştir.

Çin devleti, siber güvenlik konusunda tartışmaya açık bir takım yaptırımlara sahiptir. Örneğin; 2009 yılında Çin tarafından pornografik siteleri engellemek amacıyla Green Dam adlı yazılım geliştirilmiş, birçok yerde kullanılmaya başlanmıştır. Ancak bir süre sonra programın pornogrofik sitelerin yanında eleştirel siteleri de engellediği tespit edilmiş ve gelen tepkiler üzerine yazılım geri çekilmiştir.

Yine bu amaçla 2009 yılından beri Çin'de hack araçlarının dağıtımı ve paylaşımı suç sayılmaktadır. Kötü niyetli yazılım ve siteleri engellemek amacıyla .cn uzantılı sitelerin satın alınabilmesi için kimlik bilgisi ve lisanslı bir işletme kaydına (ICP) sahip olmak gerekmektedir. Hatta birçok siteye giriş için kimlik numarası gerekmektedir. Güvenlik açısından kimlik bilgisi almak mantıklı olsa da lisansa sahip olmadan cn.uzantılı site alınamaması gelişimi kısıtlayıcı bir etken olarak nitelendirilebilir. Ayrıca telekomünikasyon hizmeti sağlayan şirketler ile internet servis sağlayıcılara devlete ait sırları paylaşanların kimliklerini paylaşma zorunluğu getiren, internet sitesi yönetmek için regülatör ile yüz yüze görüşmeyi şart koşan bir kanun yürülüğe koymuştur. Ülkede siber güvenliğin sağlanması amacıyla çalışma yürüten bir diğer yapı internet polisidir. Bu yapı her ne kadar güvenlik zaafiyetini engellemek amacıyla kurulmuş olsa da, ifade özgürlüğü konusunda tartışmaya açık bir konumda bulunmaktadır.

Çin devletinin, hassas verilerin/gizli bilgilerin ülke dışına çıkmasını engellemekle kalmayıp; ülke içine girmesi sakıncalı olacak bilgilerin de internet ağına girmesini engelleyen meşhur firewall'u Altın Kalkan (Golden Shield Project), olası bir siber savaş durumunda Çin'e büyük avantajlar sağlayacak özelliklere sahiptir.[22] Altın Kalkan, Çin Sosyal Güvenlik Bakanlığı tarafından 2003 yılında hayata geçirilen internet gözetim projesidir. Sistem, ses ve yüz tanıma, kapalı devre televizyon, akıllı kartlar, kredi kayıtları ve internet gözetim

[22]İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü. "Siber Güvenlik Raporu" (2012, Mayıs).Erişim tarihi: 10.11.2015

teknolojilerini içeren devasa bir çevrimiçi veritabanı oluşturarak ülke içinden belirli adresleri engelleme ve ülke dışından da belirli adreslerden veri girişini engelleme temelinde çalışmaktadır. Engelleme yöntemi olarak, IP adresi engelleme, DNS filtreleme, URL filtreleme, paket filtreleme gibi yöntemler kullanılmaktadır.[23]

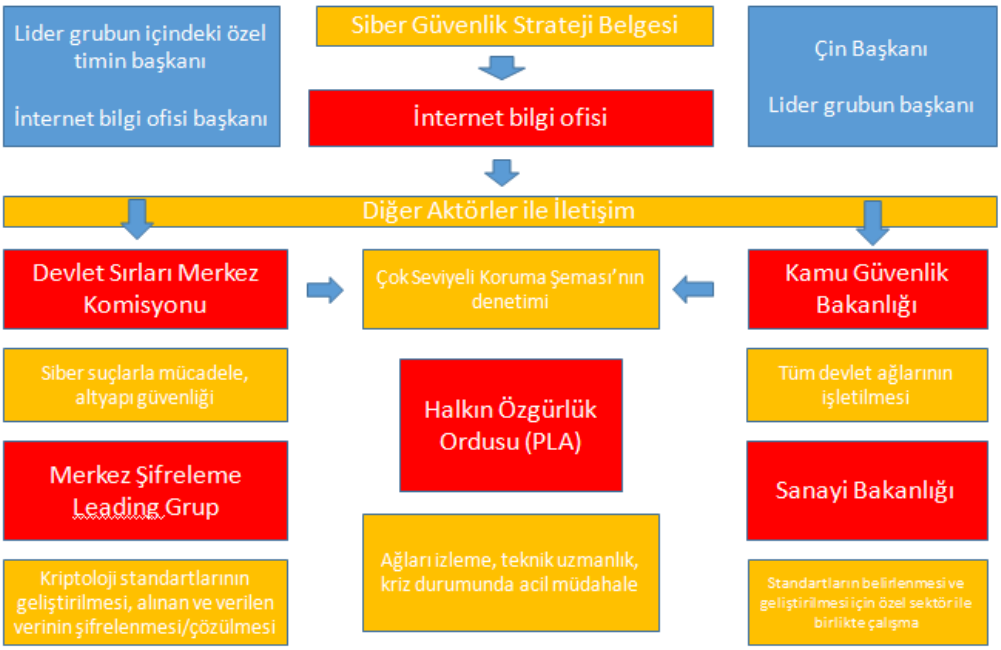
Her ne kadar Hindistan, Almanya, İran, Kuzey Kore, Pakistan, Rusya ve ABD'nin de siber saldırı konusunda hazırlıklar yaptığı tahmin edilse de Çin'in özellikle ABD'ye sürekli olarak siber saldırılarda bulunduğu belirtilmektedir. ABD siber güvenlik uzmanları ABD'nin hassas sistemlerine yapılan saldırıların Çin Ordusu kaynaklı olduğunu belirtmektedir.Kaspersky Lab firması ise yayınladığı bir raporda Çin kaynaklı hackerların toplanda 40 ülkeden 350 adetten fazla kurbana siber saldırı gerçekleştirdiğini belirtmektedir.Çin'e yöneltilen en ilginç suçlamalardan biri Gmail'in merkezine yapılan hacker saldırıdır. Bu saldırıyı ilginç yapan, Gmail'e saldıran bilgisayarların IP'lerinin Çin'de eğitim veren, başarı düzeyi yüksek olmayan bir meslek lisesine ait olması. Shandong Lanxiang Meslek Lisesi (Shandong Lanxiang Vocational School) adındaki bu lisede aşçılık, kuaförlük gibi zanaatlarin yanından bilgisayar eğitim de verilmektedir. Hayli donanımlı bir bilgisayar laboratuvarı olan bu okulun PLA desteğiyle açıldığı ve asıl amacının ordu içindeki siber güvenlik uzmanlarının çalışma yapması olduğu iddia edilse de, bu iddianın gerçekliği kanıtlanamamıştır. Saldırı yapan bilgisayarların IP'lerinin bu okulu göstermesi, zombi olarak kullanıldıklarını akla getirmektedir.[24] Çin, siber güvenlik konusunda ilk adımı 2003 yılında yayınladığı "National Coordinating Small Group for Cyber and Information Security" ismiyle bilinen ilk siber güvenlik bildirisiyle atmıştır. Bu bildiriyi 2012 yılındaki ikinci bildiri takip etmiştir. Bu bildiriye göre siber güvenlikteki temel hedefler şu şekildedir:

- Siber güvenlik teknolojisinde gelişim sağlanması,
- İnternetteki yayınların kontrol edilmesi,
- Gelecek jenerasyon mobil araçların araştırılması(5g),
- E-devlet servislerinin artırılması ve güvenliğinin sağlanması,

[23]https://en.wikipedia.org/wiki/Golden_Shield_Project
[24]Watts, Jonathan. "Gmail hack: phishing finger pointed at China's Lanxiang vocational school" (2011, 2 June). Erişim tarihi: 10.12.2015. http://www.theguardian.com/technology/2011/jun/02/chinese-school-implicated-cyber-attacks

- Kritik yapıların (doğalgaz,elektrik vb.) güvenliğinin sağlanması,
- Kriptografi standartlarının siber güvenlik kurallarına göre geliştirilmesi.[25]

Siber güvenlik alanında yapılan çalışmalar kapsamında Central Cyber Security and Informatization Leading Group (Merkez Siber Güvenlik ve Lider Grubu) kurulmuştur.Bu grubun yapısı şekil 2'deki gibidir ve siber güvenlik alanında çalışan kurumlar arasındaki koordinasyonu sağlar.



Şekil 2: Çin'de siber güvenlik uygulamaları organizasyon şeması[26]

Bu grup koordinasyonu sağlarken Çok Aşamalı Güvenlik Şeması (MLPS) adı verilen bir şema kullanmaktadır. Şema, ülkede yapılan IT çalışmalarını güvenlik seviyelerine göre kategorize eder. Tablo 1'de seviyeleri görülen MLPS sistemine göre, küçük firmalar ve kişisel kullanıcılar 1.ve 2. seviye, finans gibi stratejik önemi olan sektörler 3. seviye, devlet kurumları 4. seviye güvenlik kriterleri uygulanmaktadır. Uygulanan bu regülasyonlar nedeniyle batı firmaları Çin'de satış yapamamaktadır. Windows, Kaspersky ve Symantec gibi firmalar

[25]China Monitor. "Cyber Security in China: New Political Leadership Focuses on Boosting National Security" (2014, Aralık). Erişim Tarihi: 05.12.2015. http://www.merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf

[26]Orijinal çizim için bknz. China Monitor. "Cyber Security in China: New Political Leadership Focuses on Boosting National Security" (2014, Aralık). Erişim Tarihi: 05.12.2015. http://www.merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf

3.seviyedeki kısıtlamalardan ötürü Çin'de herhangi bir varlık göstermemektedir. Çin, bilinçli olarak uluslararası teknik anlaşmaların dışında kalmaktadır. Bunun yanında Twitter, Facebook ve Youtube yerine ülke içinde bu sitelerin benzerlerinin geliştirilmesine destek olunarak, bu sitelerin kullanılmaması sağlanmaktadır. Diğer ülkelere paralel IT standartlarını ve alternatif mobil telekomünikasyon teknolojileri kendisi geliştirmektedir. Ülkenin bu tavrı ve uyguladığı sıkı MLPS şema seviyeleri nedeniyle, zaman zaman teknolojinin gerisinde kalmakta ve insanların teknolojinin gelişimi ile ortaya çıkan önemli fonksiyonları kaçırmasına neden olmaktadır.

No	Güvenlik temelli IT ürünü kriterleri
1	Çin vatandaşları veya yasal kurumlar tarafından ulusal katılımla geliştirilen ürünler
2	Çin'in fikri mülkiyetine sahip olduğu teknolojik bileşenler
3	Üretim sürecinde sabıka kaydı olmayan kişilerin yer aldığı ürünler
4	Açık kapı (güvenlik açığı) veya Truva atı bulunmayan ürünler
5	Ulusal güvenlik ve kamu düzeni için herhangi bir risk bulundurmayan ürünler
6	Ulusal güvenlik kriterlerine göre sertifikalandırılmış yazılımlar

Tablo 1: Çin'de Uygulanan Çok Aşamalı Güvenlik Şeması (MLPS)[27]

V. Rusya ve Siber Güvenlik Uygulamaları

Rusya, siber faaliyet hacmi açısından tüm dünyada ABD ve Çin'in ardından 3.sıradadır. Buna rağmen, en yetenekli hackerların Rusya'nın hackerları olduğu kabul edilmektedir. Bu durumun şaşırtıcı olan yanı, Çin hükümeti hackerları açıkça detseklemek ve ordu içerisinde çalıştırarak işbirliği yapmakta olmasına, Rusya hükümetinin bu tarz bir çalışması olmamasına rağmen, hackerların bu derece ileri gidebilmesidir.

[27]Orijinal çizim için bknz. Orijinal çizim için bknz. China Monitor. "Cyber Security in China: New Political Leadership Focuses on Boosting National Security" (2014, Aralık). Erişim Tarihi: 05.12.2015. http://www.merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf

Rusya, sıklıkla diplomatik ilişkilere paralel olarak meydana gelen siber saldırılar nedeniyle suçlanmaktadır. Örneğin; 2008 yılında yaşanan Rusya-Gürcistan Savaşı sırasında bilindik seyrinde devam eden fiziksel savaşa, daha fiziksel savaş başlamadan önce başlayan siber savaş eşlik etmiştir. Diplomatik gerginlik sırasında Gürcistan devlet başkanının sitesine yapılan DDoS saldırıları, savaşın başlaması ile ülkedeki birçok siteye yönelmiştir. Bu saldırılar, ülkeye fiziksel veya maddi hiçbir zarar vermemiş; ancak savaş sırasında Gürcistan Hükümeti'ni zayıf düşürmüş ve ülkedeki haberleşmeyi zaafiyete uğratmıştır.[28] Rusya, hiçbir zaman siber saldırı yaptığını açıklamamış olsa da, hackerlar ile stratejik ilişiler içinde olduğu her zaman düşünülegelmiştir.

Rusya'nın siber uzaydaki aksiyonları ile ilgili yaşanan ikinci örnekse 2007 yılında Estonya'nın uğradığı ve 1 ay süren siber saldırılar olacaktır. Bu saldırıların da tıpkı Rusya - Gürcistan Savaşı'nda olduğu gibi Rusya ve Estonya arasındaki bir diplomatik anlaşmazlıkla aynı döneme denk gelmesi ve saldırıyı Rus bir hacker grubun üstlenmesi, Rusya'nın bu tarz eylemleri desteklediği yönündeki savları güçlendirmektedir.[29] Bu gibi örneklerde üzerinde düşünülen önemli noktalardan biri, siber güvenlik konusunda yaşanan eleman açığına rağmen Rusya'nın nasıl bu istihdamı sağladığıdır? Devlet için çalışan hackerlar, bunu vatanseverlik mottosuyla yaparken; siber suçlular diyebileceğimiz kategoride çalışan hackerlar, maddi kazanç elde etmek için yapmaktadırlar. Vatanseverlik mottosuyla siber saldırılar düzenleyen kişilerin istihdamı da ya Çin'deki gibi devlet memuru hackerlar aracılığı ile ya da Rusya örneğindeki gibi direkt kanunlar aracılığı ile bir bağlantı olmadan yani paramiliter şekilde çalışan hackerlar ile olmaktadır. Tüm bu anlatılanlara rağmen Rusya örgütlü ve oturmuş bir siber sistem oluşturmuş değildir. Siber güvenlik alanında son birkaç yıldır atılım yapmaktadır ve çalışmaları henüz temel safhadadır.

Rusya ilk siber güvenlik statejisinin temellerini 2000 yılından beri atmış olmasına rağmen bugüne kadar yapılan çalışmalar çok güçlü bir siber güvenlik organizasyonu oluşturabilmiş değildir. Bununla birlikte, 2012 yılında oluşturulan ilk siber staratejinin ardından, 2014 yılından itibaren bu alanda yapılan çalışmalara artan bir ivmeyle devam edilmektedir. Şu an gelinen noktada, Rusya

[28]Bakır, Emre. "5. Boyutta Sacaş: Siber Savaşlar – I" (2012, 20 Aralık). Erişim tarihi:21.12.2015. https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-i.html

[29] Estonya'ya yapılan siber saldırı, Estona incelemesinde ayrıntılı olarak anlatılacaktır.

devleti Rusya Savunma Bakanlığı çatısı altında 2015 yılı başında siber saldırı karşılık merkezi[30] kurma çalışmalarına başlamıştır. Bu merkezin siber saldırılarla mücadele etme görevinin yanı sıra, 7/24 mantığında çalışarak ulusal siber uzaydaki aktiviteleri izlemek ve analiz etmek görevini de yütümesi planlanmaktdır. Bu merkezin oluşunda Çin'i örnek aldığını bildiren Rusya İletişim Bakanı, söz konusu merkezin topluma siber güvenlik farkındalığı kazandırmak ve liselerde yazılım eğitimleri verilmesinin koordine edilmesi sorumluluğunun da verileceğini belirtmektedir. Siber strateji planının en önemli maddelerinden biri de kritik yapıların siber saldırılardan korunmasının sağlanmasıdır. Ülkedeki su ve ısınma altyapıları, trafik ışıklarının kontrolü ile nükleer ve hidro elektrik santral sistemlerinin korunması için çalışmalar yürütülmesi planlanmaktadır.

Rusya, her ne kadar kamu kurumları içinde siber güvenlik alanındaki çalışmalarının çok başında olsa da sahip olduğu hacker potansiyeli nedeniyle siber güvenlik ve siber savaş alanında geleceğin önemli bir aktörü olmaya aday gösterilmektedir.[31] Bu resmi olayan hacker gücünün askeri alan ile birleştirilmesi, ülkenin siber savunması açısındanda, diğer ülkeler için siber tehdit oluşturma potansiyeli açısından da önemli bir hamle olacaktır. Nitekim, 2013 yılında yaptığı bir açıklama ile 2014 yılında ordu içerisinde siber güvenlikten sorumlu bir birim oluşturulmaya başlanacağını ve 2017 yılına kadar bitirilmesinin hedeflendiği belirtilmiştir. Bu amaçla, 2014 yılından itibaren IT uzmanı alımı ve yeni mezun bilgisayar mühendislerinin askeri birim içerisinde çalışmak üzere istihdam edilmesine başlanmıştır.

Mevcut sistemde, siber saldırıların takibini Rusya Federal Güvenlik Servisi (FSB) yürütmektedir. Ayrıca ülke, üç adet CERT birimine de sahiptir. Bu birimler, devlete ait olan RU-CERT ve GOV-CERT.RU ve özel şirketlerin liderlik ettikleri özel bir CERT kurumu olan CERT-GIB adlı birimlerdir. Bu birimler, 7/24 ülke ağlarını kontrol etmek ve herhangi bir saldırı drumunda karşılık vermek veya savunma yapmak amaçlı çalışmaktadırlar. Ayrıca, siber güvenlik konusunda ülkedeki kurumların koordinasyonunu sağlamak, teknik ve hukuki anlamda destek vermek, saldırı durumunda uyarı oluşturmak, siber saldırı konusundaki ihbarları almak ve değerlendirmek, siber saldırıları analiz etmekten de sorumlulardır. Bu

[30]Cyber-Threat Response Centre
[31]Yener, Yavuz. "Rus Krizinin Gözden Kaçan Boyutu: Siber Savaş Tehdidi" (2015, 2 Aralık). Erişim tarihi: 10.12.2015.
http://www.usak.org.tr/analiz_det.php?id=17&cat=365366706#.VofHRPkaaT9

kurumların dünyadaki diğer CERT kurumlarıyla herhangi bir işbirliği bulunmamaktadır. Ancak Rusya ile Çin arasında 2015 yılı Mayıs ayında bir siber güvenlik anlaşması imzalanmıştır. Bu anlaşmaya göre, "iki ülke, birbirine siber saldırıda bulunmayacak ve internet güvenliği üzerine birlikte hareket edecek. Oluşabilecek tehditlere karşı birbirlerini bilgilendirecek ve çözüm bulmaya çalışacaklar."[32]

VI. NATO ve Siber Güvenlik Uygulamaları

Siber güvenlik ve siber risk kavramlarının NATO nezdinde dikkat çekmesi 1999 yılına denk gelmektedir. NATO'nun 1999 yılında Kosova'ya yaptığı müdaheleye tepki göstermek amaçlı NATO sistemlerine yapılan ufak çaplı saldırılar NATO'nun dikkatini siber savunma konusuna çekmesine neden olmuştur. Başlangıç olarak Kosava'ya yapılan müdahale gösterilse de birçok kaynağa göre siber güvenliğe olan bakış açısını asıl değiştiren olay 11 Eylül 2001'deki İkiz Kule saldırısıdır.[33] 11 Eylül olayından 1 sene sonra 2002 Prag Zirvesi'nde siber güvenlikle ilgili ilk kararlar alınmıştır. NATO, kendini siber saldırılarla baş edebilecek seviyeye getirme kararı almıştır ancak bu karar hemen hayata geçirilememiştir. NATO'nun siber güvenlik alanındaki üçüncü mihenk taşı ise 2007 yılında meydana gelen Estonya siber saldırısı olmuştur. Bu sadırılar ile NATO siber savunma alanında ne kadar zayıf olduğunu fark etmiş ve bu nedenle 2008 yılında NATO Müşterek Siber Savunma Mükemmeliyet Merkezi'ni (NATO CCD-COE) ve Siber Savunma Yönetim Otoritesi'ni (CDMA) kurmuştur. CDMA, siber savunma koordinasyonu, kapasitelerin denetimi ve risk yönetimi konularında görevlendirilirken; CCD-COE, siber güvenlik bilimi ve eğitimi, NATO sistemleri arasında uyum ve hukuki sorunlar, NATO'nun siber yetkinliklerinin geliştirilmesi gibi konularda çalışmalar yaparak NATO'nun siber uzaydaki operasyonel gücünün desteklenmesi amacına hizmet etmeye başlaşmıştır.[34]CCD-COE 'de NATO üyesi ülkelerden çalışanlar da bulunmaktadır. 2008 yılında ayrıca 3 temel maddeden oluşan "NATO Siber Savunma Politikası" oluşturulmuştur. Bu üç madde aşağıda özetlendiği gibidir:

---

[32] wall-street-journalın haberi

[33]"Yeni Tehditler: Siber Boyut" Erişim tarihi: 10.12.2015. http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/TR/

[34]Yener, Yavuz, "NATO ve Siber Güvenlik 2 – Strateji" (2014, 27 Aralık). Erişim tarihi: 11.12.2015. http://siberbulten.com/makale-analiz/nato-ve-siber-guvenlik-2-strateji/

- **Yerinde hizmet**, Yardım talep üzerine sağlanır; aksi takdirde egemen devletlerin kendi sorumluluğu ilkesi yürürlüktedir.
- **Yinelememe**, Uluslararası, bölgesel ve ulusal düzeylerde yapıların veya yeteneklerin gereksiz yere tekrarlanmasından kaçınılır.
- **Güvenlik**, Güvene dayanan, erişime açılması gereken sistemle ilgili bilginin hassasiyetini ve olası zayıf noktaları göz önünde bulunduran işbirliği oluşturulur.[35]

NATO'nun 2010 yılı stratejik raporunda siber saldırılara karşı önlem alma, saldırı tespiti ve engellemeye yönelik çalışmalar yapılması planlanmış; ayrıca Bilgisayar Olaylarına Müdahale Yeteneği gibi mevcut yapılarını güncellenmesine karar verilmiştir. Yine aynı yıl yapılan Lizbon Zirvesi'nde Siber Savunma Politikası dokümanının oluşturulması kararı alınmıştır. 2011 yılında NATO Siber Savunma Politikası ve Eylem Planıkabul edilmiştir. Eylem planının öne çıkan maddeleri şunlardır:

- Teknolojinin gelişimi ile birlikte ittifakın devamı için gerekli olan en önemli unsurlardan biri de siver savunma olmuştur. Nato'nun nihai hedefleri olan kollektif savunma ve kriz yönetimi gelinen noktada siber güvenlik olmadan mümkün değildir.
- NATO ve müttefiklerinin siber saldırılara karşı direnci artırılmalı ve gerektiğinde destek olunmalıdır. Kritik verilen siber saldırılara karşı korunması ve saldırı durumunda ortaya çıkan hasarın da kısa sürede giderilmesi NATO'nun hedefleri arasındadır.
- NATO ağları tek bir merkezde yönetilmelidir.
  - ✓ Ağların tek bir merkezden yönetilmesi fikri, olası bir saldırıda tüm sistemin tehlikeye atılması anlamına gelmesi yönüyle eleştirilmektedir.
- NATO üyesi tüm devletlerin sahip olması gereken minimum siber savunma yeteneği seviyesi belirlenmelidir.
- NATO üyesi tüm devletlere, sahip olunması gereken minimum siber savunma seviyesine ulaşabilmeleri için NATO tarafından destek verilmelidir.

[35]"Yeni Tehditler: Siber Boyut" Erişim tarihi: 10.12.2015. http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/TR/

- ✓ Bu sayede kritik altyapıların korunmasına öncelik verilerek can ve mal kaybını en aza indirmek, ayrıca müttefik devletler arasında tecrübe paylaşımına imkan sağlamak isteniyor.

- Ortak devletlerle, uluslararası örgütlerle, özel sektörle ve akademiyle işbirliği sağlanmalıdır.
  - ✓ Siber uzayda ulusal ve uluslararası işbirliğinin önemi tekrar vurgulanmış durumda. Uluslararası örgütler, belli standartların oluşturulabilmesi açısından çok hayati bir işleve haiz. Özel sektör, saldırılardan en çok zarar gören ve siber istihbarat anlamında en çok hedef alınan şirketleri içinde barındırıyor. Akademi ise siber güvenliğin bilimsel boyutunu açıklama işini üstleniyor. NATO'nun bu üç alanda oynayacağı rol ile, tüm tarafların kazançlı çıkacağı bir ilişkiler zinciri oluşturmak isteniyor.[36]

NATO, müttefikleriyle yürüttüğü çalışmaların kesintisiz bir şekilde devam etmesini amaçlamakta ve bunun için de siber savunma alanında çok iyi bir noktada olunması gerektiğinin bilincindedir. Bu amaçla hem teknik olarak güçlü sistemler inşa etmek hem de sürekli gelişen ve değişen teknolojinin ve savunma tekniklerinin takibini sağlamak, bu sayede kendi sistemlerini güncel tutmak amaçlanmaktadır.

NATO tarafından tüm üye ülkeleri koordine etmek için NATO Defence Planning Process (NDPP) yapısı; saldırılara cevap vermek için NATO Computer Incident Response Capability (NCIRC) yapısı kurulmuştur. NCIRC, 2003 yılında oluşturulması planlanan ve 2006'dan bu yana NATO bilgisayar ağlarına yapılan ataklarla mücadele etmekte olan bir kurumdur. NATO'nun siber güvenlik alanındaki atılımlarının en önemli noktası, tüm çalışmalarının "savunma" yeteneği üzerine yapılmasıdır. Ülkeler ise kendi siber güvenlik çalışmalarını, hem savunma hem saldırı alanında gelişim sağlama amacına yönlendirmiş durumdalardır.

[36]Yener, Yavuz, "NATO ve Siber Güvenlik 2 – Strateji" (2014, 27 Aralık). Erişim tarihi: 11.12.2015. http://siberbulten.com/makale-analiz/nato-ve-siber-guvenlik-2-strateji/

VII.Almanya ve Siber Güvenlik Uygulamaları

Almanya, siber güvenlik yarışına daha önce anlatılan ülkelerden geç başlamıştır. İlk ulusal siber güvenlik stratejisini 2011 yılında oluşturmasına rağmen, hızlı gelişme göstermiş ve 2015 yılında stratejisini yenileyerek yola devam etmektedir. Almanya, oluşturduğu stratejilerde kritik alt yapıların korunması konusunu öne çıkarmaktadır. Ayrıca internet kullanımının artmasıyla her ülkenin sadece kendi sistemlerinde değil; başka ülkelerin sistemlerinde meydana gelen saldırılardan da etkilenebilceği global bir dünya oluştuğundan, bu nedenle de siber güvenlik ve siber savunma mekanizmalarının uluslararası düzeyde olmasının öneminde bahsedilmektedir. Hatta kanunen de bu gibi bir düzenlemeye gidilmesi gerektiği belirtilmektedir. Hem Birleşmiş Milletler, Avrupa Birliği, NATO, G8, OSCE ve diğer uluslararası örgütlerin birlikte çalışması gerektiğini vurgulamaktaıdr.

2011 yılında oluşturulan stratejinin 10 maddesi özetle şu şekildedir:

- Kritik yapıların ve bilgi sistemlerinin korunması
- IT sistemlerinin güvenilir hale getirilmesi: Özellikle siber saldırıların ilk hedefi olan vatandaşların ve küçük ölçekli şirketlerin güvenliğinin sağlanması. Siber güvenlik konusunda toplumu bilgilendirmek amacıyla ortak bir insiyatif kurulması. Devlet tarafından, özel kuruluşların standartlara uyup uymadıklarının belirlenmesi ve güvenlik standartlarına uygun hizmet vereye tesşvik edilmesi.
- Devlet kurumlarında IT sistemlerinin güvenliğinin sağlanması: Kamu kurumarından sistemlerin korunmasının ve veri güvenliğinin sağlanması. Ülke içinde kullanılacak ortak bir federal ağ oluşturulması. Siber savunma yapısında kurumlar arası iletişim yapısının oluşturulması. Almanya CERT kurumunun, bu konuda insyatif kullanması.
- Ulusal Siber Müdahale Merkezinin kurulması: Meydana gelecek bir saldırıda tüm kurumlar arası koordinasyonun sağlanmasından ve müdahale edilmesinden sorumlu bir Ulusal Siber Müdahale Merkezi kurulacaktır. (National Cyber Response Centre) Ülkedeki siber güvenlikle ilgili sorumluluk sahibi tüm birimler bu kurum altında

toplanacaktır. (The Federal Criminal Police Office (BKA), the Federal Police (BPOL), the Customs Criminological Office (ZKA), the Federal Intelligence Service (BND), the Bundeswehr ve kritik altyapıların opertorleri) Kurum, olası bir saldırıda hızlı bilgi paylaşımı sağlamak, zaafiyetlerin ve saldırganlara iat bilgilerin paylaşımını sağlamak ve tavsiye vermekte sorumludur.

- Ulusal Siber Güvenlik Konseyi'nin kurulması: Kamu kurumları ile özel sektöre arasında iletişimi sağlayan ve olası bir krizde/saldırıda nedenini belirleme ve ortadan akldırma noktasında önemli rolü olacak bir yapı oluşturulacaktır. Bu yapıda Dışişleri Bakanlığı, içişleri bakanlığı, savunma bakanlığı, ekonomi ve teknoloji bakanlığı, Adalet bakanlığı, maliye bakanlığı, eğitime ve araştırma bakanlığından temsilerin olması planlanmaktadır. Interdisipliner şekilde çalışacak bu yapıda kamu-özel ortaklığnını sağlanması planlanmaktadır.
- Siberuzayda suçların kontrol edilmesinin sağlanması: Kolluk kuvvetlerinin ve kamu kurumundaki bu alanda çalışanların yeteneklerinin artırılması gerekmektedir. Diğer ülkelerle dayanışma yapılacak ve eksiklerin giderilmesi sağlanacaktır.
- Siber güvenliği sağlamak için avrupa ve tüm dünya ülkelerinin güçlerini birleştirmesi: European Network and Information Security Agency (ENISA) direktifinin sürdürülmesi ve mümkün olduğunca çok ülkenin katılımıyla ortak bir siber kanun hazılanması gerekmektedir.
- Güvenilir teknolojilerin kullanımı: Özellikle kritik yapılarda kullanılan yazılımların, güvenliğinin stadardize edilmesi.
- Kamu kurumlarındaki personelin eğitimi: Kurumlarda siber güvenlik alanında teknik eleman ihtiyacının analiz edilmesi, gerekirse kurumlar arasında personellerin değiştirilmesinin sağlanması.
- Saldırılara karşılık verecek araşların niteliği: Siber saldırılara cevap verebilmek için etkili ve güvenliği sağlanmış savunma araçlarının ve sistemlerinin bulundurulması şarttır.

Gelinen noktada Almanya'da kritik yapıların siber tehditlerden korunmasından ve bu konudaki çalışmaların koordine edilmesinden sorumlu birim, Bilgi Güvenliğ Federal Ofisi'dir. (BSI) 2011 yılında hazırlanan stratejik plandan 4 yıl sonra, 2015 yılında çıkan siber güvenlik yasasında yer alan maddeler ile birlikte, BSI'nın etkinliği de artmıştır. Bu yasaya göre Almanya'nın en çok önem verdiği alan olan kritik altyapıların korunması için bu yapıları işleten bankalar, enerji şirketleri, hastaneler gibi özel şirketlere, minimum seviyede uyulması gereken bilgi güvenliği standartlarını belirtilmekte ve siber güvenlik standartlarına uymamaları halinde 100 bin avroya kadar ceza verilmesi öngörülmektedir. Kanunla birlikte şirketlerin sistemlerini siber güvenlik standartlarına göre güncellemesi için 2 sene süre verilmektedir ve bu sürenin sonunda tüm şirketler 2 senede bir BSI tarafından denetlenecektir. Sözkonusu şirketler herhangi bir siber saldırı durumnda bunu BSI'ya bildirmek zorunda olacaktır. BSI, bu durumda saldırıyı inceleyecek ve diğer şirketleri uyaracaktır. Ayrıca telekom şirketlerine, müşterilerinin internet ve telefon bağlantıları istismar edildiğinde bunu müşterilere bildirme zorunluğu getirilmektedir. Bunun yanı sıra, siber suçlarla mücadeledeki gücünü artırmak için polis kuvvetlerine ciddi yetkiler veren kanun, bu yönüyle tartışma yaratmıştır. Yasa, telekom şirketlerine müşterilerinin data trafiğini, gerektiğinde polis tarafından kullanılması amacıyla, 6 ay boyunca saklamasını zorunlu tutmaktadır. Bu madde yönüyle yeni kanun eleştirilirken; diğer yandan Almanya hükümeti kişisel verilen korunması için çalışan birimi tek başına bir kurum haline getirerek, veri korumanın daha etkin bir şekilde sağlanması, sistemin gelişen teknoloji ile uyumlu şekilde çalışması ve doğrudan hükümete bağlı bir kurum olarak görev yapması için çalışmaktadır.

Almanya'nın 2015 yılında yaptığı bir diğer atılım ise ordu içinde bir Bilgi teknolojileri birliğinin kurulması için çalışma başlatmak olmuştur. Ordu, hali hazırda siber güvenlik alanında çalışan personel bulundursa da çok daha yetenekli 15 bin kişilik bir siber birim kurulması planlanmaktadır. Siber ordu kurma konusunda diğer birçok ülkeden geç kalmış olan Almanya'nın hedefinin, saldırı değil; savunma amaçlı bir ordu kurmak olması dikkat çekicidir.

Şekil 3: Almanya'da siber güvenlik organizasyon yapısı[37]

VIII. Estonya ve Siber Güvenlik Uygulamaları

Estonya siber güvenlik alanında yapılan her çalışmada muhakkak adı geçen bir ülkedir. Bunun sebebi siber güvenlik kavramının yeni oluştuğu yıllarda uğradığı siber saldırı ile siber güvenlik konusuna bakış açısını değiştirmesi ve belki de bugün gelinen noktada bir mihenk taşı olmasıdır. Bu saldırılar bugün ilk siber savaş olarak bilinir.

2007 yılında Estonya'nın Tallin Meydanı'ndaki Bronz Asker Anıtı'nı kaldırması ile başlayan bir siber saldırı ağı, ülkenin sistemlerini 3 hafta boyunca felce uğratmıştır. Bunun en temel sebebi dönemin hükümetinin ülkenin sistemlerini teknolojik hale getirmeyi hedeflerken, bu teknolojik sistemlerin güvenliğini es geçmesi olmuştur. Saldırıların olduğu dönemde Estonya vatandaşları, gündelik hayatlarının büyük kısmında internete bağımlı idi. Ayrıca bankacılık işlemlerinin çok büyük bir kısmı internet üzerinden yapılıyordu. Yine o dönem ilk defa elektonik oy kullanımı Estonya'da yapılmıştı. Ülkeye yapılan DDoS saldırıları, öncelikle siyasi partilerin internet sitelerini, ardından yayın organlarının sitelerini ve üçüncü dalga olarak bankacılık sistemini kilitlemiştir. Hazırlıksız yakalanan Estonya, NATO'dan yardım istemiş ve NATO uzmanlarının desteği ile saldırılar atlatılabilmiştir. Ülkedeki siber güvenliğin, teknolojik gelişmelere paralel ilerlememesi sonucunda bugün hala konuşulan

[37]Orijinal çizim için bknz. Güngör, Murat. "Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma" (2015, Mart

saldırılar Estonya'da büyük izler bırakmıştır.Bununla birlikte Estonya, NATO ve diğer birçok ülkenin siber güvenliğin önemini fark etmesine ve önlemler almaya başlamasına neden olmuştur. Estonya bu olaydan hemen sonra ilk siber güvenlik stratejisini oluşturmuş, NATO 2008 yılında saldırılar nedeniyle sembolik bir önem kazanan Tallinn'de, NATO üyesi ülkelere siber güvenlikte destek vermesi ve iş birliğini sağlaması ayrıca siber güvenlik araştırmaları yapması amacıyla bir Siber Güvenlik Mükemmeliyet Merkezi kurmuştur. Ayrıca NATO, bu saldırılardan sonara üye ülkeleri siber güvenlik stratejisi oluşturmak konusunda teşvik etmiş, ve ülkelerarası işbirliği için çalışmaya başlamıştır.

Estonya, 2007 yılından bu yana siber güvenlik alanında birçok gelişim yaşamıştır. İlk olarak Siber Güvenlik Strateji Komitesi[38] kurulmuş ve siber güvenlik stratejisi bu komite tarafından hazırlanmıştır. Komite, Savunma Bakanlığı, Dış İşleri Bakanlığı, İç İşleri Bakanlığı, Eğitim ve Araştırma bakanlığı, Adalet bakanlığı ve Ekonomi bakanlığından oluşmaktadır. Komite tarafından alınan kararlar, Siber Güvenlik Konseyi tarafından uygulanmaktadır. Estonya bu alanda hem yönetsel reformlar geliştirmekte hem siber güvenlik alanında uzmanlığını artırmakta hem de ülkeler arası işbirliği için çalışmaktadır. Ülkeler arası işbirliğini önemini yaşayarak anlayan Estonya'nın bu tavrından ders çıkarılmalıdır.

Estonya'nın bir diğer önemli kurumu, Kritik Altyapıları Koruma Şubesi (CIIP)'dir. Bu şubenin görevi, su, elektrik, doğalgaz vb. kritik öneme sahip ağların güvenliğini sağlamaktır. Ayrıca risk değerlendirme ve savunma alanında çalışmalar yapılmakta; acil eylem planı oluşturma, su elektrik gibi sistemlerin işletmecilerine güvenlikle ilgili tavsiyelerde bulunma ve destek verme gibi projeler yürütülmektedir.

Siber güvenlik alanında güçlü sayınan diğer ülkeler gibi Estonya'nın da bir CERT kurumu bulunmaktadır. CERT-EE, 2008 yılında kurulmuştur. Ülkedeki siber saldırıları takip etmek, tespit etmek ve saldırı altındaki sitelere veya sistemlere teknik destek vermekten sorumludur. Estonya'nın siber saldırı tespit sistemi de Cert-EE tarafından kullanılmaktadır.

Estonya'da siber güvenlik desteği veren bir başka kuruluş ise 2011 yılında kurulan Estonya Bilgi Sistemi Otoritesi'dir. (EISA) Bu kurumun amacı, kamu

[38] Cyber Security Strategy Committee

kuruluşları ve özel şirketlere bilgi sistemlerinin güvenliğini sağlamaları konusunda destek vermek ve ülkedeki siber atakları takip etmektir.

Bugün Estonya e-ülke (e-country) olarak bilinir ve kamu hizmetlerinin %95'i web servisler üzerinden sağlanır. Estonya, şu an siber saldırılara en hazırlıklı ülkelerden biridir. Ayrıca Estonya'da 2007 yılından beri, kamu-özel sektör ortaklığı sürdürülmektedir.

2010 yılında Estonya'da Siber Güvenlik Ligi[39] adında Savunma Bakanlığı tarafından yürütülen bir gönüllülük programı kurulmuştur. Ülkenin önde gelen şirketlerinde çalışan hukukçular, programcılar, bilgisayar bilimciler ve yazılımcılardan oluşan bu ligde farklı sektörlerde farklı kurumlarda çalışan uzmanlar bir araya gelerek, muhtemel siber saldırılara karşı egzersizler yapmaktadır ve olası bir saldırıda gönüllü siber orduyu oluşturmaları hedeflenmektedir. Bu topluluktaki özellikle özel sektör çalışanları, özel sektörde edindikleri bilgileri, olası bir savaşta ülke adına kullanacaklardır. Ligin amaçları:

- Başarılı IT uzmanlarını bir araya getirmek,
- Kritik bilgi sistemlerinin korunma oranını artırmak,
- Kamu-özel sektör arasında bir iletişim oluşturmak ve bu sayede olası bir kriz durumunda organize olabilmeyi sağlamak,
- Topluluk altındaki kişilerin düzenli olarak siber güvenlik konusunda pratik yapmalarını sağlamak,
- Böyle bir durumda toplumun mağduriyeti en aza indirmek

olarak sıralanabilir.[40]

Estonya'nın ordu altındaki üç biriminden biri olarak sayılan defence league, ordunun siber ayağını oluşturmaktadır. Diğer ülkelerin aksine, ordu içindeki siber güçler, bir meslek değildir ve gönüllüllük esasına dayanır. Ülkedeki polis kuruluşunun da kendi altında çalışan bir siber suçlar birimi bulunmaktadır.

Ayrıca üniversitelerde siber güvenlik alanında eğitim veren birimler açılmıştır ve şirketlere siber güvenlik uzmanları yetiştirmek için çalışmalar yürütmektedirler. Bunun yanında 2015 yılında genç neslin geleceğin siber güvenlik saldırılarına karşı hazırlıklı olması için lise düzeyinde NATO işbirliği ile siber savunma sınıfları oluşturulmaya başlanmıştır. Sınıflarda siber güvenlik,

[39] Cyber Security Defence

[40] Estonian Defence League. "Cyber Defence Unit" (2015, 3 Ağustos). Erişim tarihi: 12.12.2015. http://www.eesti.ee/eng/topics/riigikaitse/vabatahtlik_osalemine_riigikaitses/kuberkaitse_uksus

kriptoloji, mekatronik ve 3D modelleme, internette güvenlik temelleri konularında eğitimler verilmektedir. Bu sınıfları tamamlayan öğrencilere Savunma Ligi'nden bir sertifika verilmektedir.[41]

Estonya, gelinen noktada olası bir saldırı durumunda hizmetlerin aksamaması için ülkenin dijital hizmetlerini bulut sistemine aktarma çalışması yapmaktadır. Dijital hizmetlerin bulut sistemine taşınmasıyla sunucuların Almanya, Hollanda, Avustralya ve Kanada'daki büyükelçiliklerde bulundurulması planlanmaktadır.

IX. İngiltere ve Siber Güvenlik Uygulamaları

İngiltere, son yıllarda siber güvenliği ülke ekonomisine eklemlendirme ve siber güvenlik olayını hem yazılım hem de donanım boyutlarıyla dünya çapında öncüsü olacağı bir alan haline getirmeyi hedeflediğini gerek Ulusal Siber Güvenlik Stratejisi'nde, gerekse uluslararası platformda sıklıkla dile getiren bir ülkedir.[42]İlk siber güvenlik stratejisini 2009 yılında oluşturmuş ve 2016 yılına kadar siber güvenlik konusunda kendini sürekli geliştirmeye devam etmiştir. 2010 yılında oluşturulan Ulusal Güvenlik Stratejisi'nde (UGS), ulusal güvenlik anlayışının 10 yıl öncesine göre çok değiştiği vurgulanmakta ve siber saldırıların kamu kurumlarına, askeri, endüstriyel hedeflere yönelmesi durumunda hayatı felç edecek etkisine dikkat çekilmektedir. Aynı yıl içinde UGS'ye ek olarak yayınlanan Stratejik Savunma ve Güvenlik Gözden Geçirme (SSGG) belgesinde ise gelecek 4 yıllık siber güvenlik bütçesi belirlenmektedir. Her iki belgede de ABD ile siber güvenlik alanında birlikte çalışılması gerektiği vurgulanmıştır. 2011 yılında yayınlanan son siber güvenlik stratejisinde İngiltere 2015 hedeflerini şu şekilde belirtmektedir:

- Siber suçlar konusunda ilerleme kaydetmek ve dünyanın siber uzayda çalışılan en güvenli ülkelerinden biri olmak.
- Siber saldırılara hızlı müdahale edebiliyor olmak ve siber uzaydaki menfaatlerimizi en iyi şekilde korumak.

---

[41]http://uatoday.tv/politics/estonia-549267.html

[42]Bozdemir, Nazlı Zeynep. "İngiltere'yi Siber Güvenlik Sektöründe Sırtlayan Adam"(2014, 8 Aralık). Erişim tarihi: 12.12.2015. http://siberbulten.com/makale-analiz/ingiltereyi-siber-guvenlik-sektorunde-sirtlayan-adam-andy-williams/

- Toplum için şeffaf ve güvenli bir siber uzay oluşturmak.
- Ülkenin tüm siber güvenlik unsurlarına, en kestirme yoldan deneyim ve yetenek kazandırmak için gerekli desteği vermek.

Ülkenin siber güvenlikle ilgili en yetkili birimi, İngiltere'nin dış istihbarattan sorumlu olan Gizli İstihbarat Servisi (MI6) ve iç istihbarattan sorumlu kurum olan Güvenlik Servisi (MI5) ile birlikte 3 büyük istihbarat ajansından bir tanesi olan GCHQ (İngiltere Hükümet İletişim Merkezi)'dir. "Kurum, İngiltere Dışişleri Bakanlığı ve Devlet Sekreterliğine bağlı olarak çalışmaktadır ve İngiltere Dışişleri Bakanı sorumluluğundadır. Ancak daimi olarak Dışişleri Bakanlığı'nın bir parçası değildir." GCHQ, dünyanın birçok yerinden gelen dijital ve elektronik sinyalleri toplar ve analiz eder ve diğer ekiplerle paylaşır.

"İngiltere Hükümet İletişim Merkezi (GCHQ), İletişim-Elektronik Güvenlik Grubu (CESG) ve Ortak Teknik Dil Servisi (JTLS) olmak üzere iki ana alt birime sahiptir. İletişim-Elektronik Güvenlik Grubu (CESG), İngiliz ulusal altyapının kritik parçalarının iletişim ve hükümet bilgi sistemlerinin güvenliğini sağlamak için çalışmaktadır. CESG kriptografi dâhil olmak üzere bilgi güvenliği için İngiltere Ulusal Teknik Makamı'dır. Ayrıca GCHQ'nun kendisi, Oxford Üniversitesi'nde ve Bristol Üniversitesi Heilbronn Enstitüsü'nde bulunan Kuantum Bilgisayar Merkezi gibi alanlardaki araştırmalara finansal destek olur."[43] Kurumun yaklaşık 6200 çalışanı vardır. Yaptığı çalışmalar hem siber güvenlik alanında hükümete ve askeri güçlere bilgi sağlamakta hem de ülkenin haberleşme ve bilgi sistemleri ile kritik altyapılarını korumaktadır.

İngiltere'nin kritik altyapıları korumaktan sorumlu ayrı bir devlet kurumu bulunmaktadır. CPNI (Center for Protection of National Infrastructure) adındaki bu kurum, siber güvenlik alanında yaşanacak saldırılara karşı da önlemler almakta ve çalıştığı kurumlara çeşitli tavsiyelerde bulunmaktadır. CPNI'nın korumaktan sorumlu olduğu alanlar, iletişim ve haberleşme, acil servisler (ambulans, itfaiye, polis, vb.), enerji, finansal servisler, gıda sektörü, hükümete ait kurumlar, sağlık, ulaşım, su olarak dokuz kategoriye ayrılmıştır.[44] Bu kurum SCADA sistemlerinin

[43]https://tr.wikipedia.org/wiki/H%C3%BCk%C3%BCmet_i%CC%87leti%C5%9Fim_merkezi
[44]http://www.cpni.gov.uk/about/cni/

güvenliği konusunda bir rehber yayınlamış ve aşağıdaki maddelere dikkat çekmiştir:

- İş risklerinin anlaşılması
- Güvenli mimarinin gerçeklenmesi
- Olayları ele alma yeteneğinin oluşturulması
- Farkındalığın artırılması ve yeteneklerin geliştirilmesi
- Üçüncü parti risklerin yönetimi
- Projelerin güvenlikle birlikte ele alınması
- Sürekli bir yönetişim modelinin kurulması

İngiltere'de bilişim güvenliği alanında eğitim/seminer verme ve sertifikalandırma alanında hizmet veren, kar amacı gütmeyen International Information Systems Security Certification Consortium ((ISC)²-ISC) adlı kurum önemli bir görevi yerine getirmektedir. Dünyanın en çok bilinen sertifikası, Certified Information Systems Security Professional (CISSP) bu kurum tarafından verilmektedir. Ayrıca dünyaca ünlü siber güvenlik eğitim kurumu Sans Institute Cyber Academy, İngiltere Savunma Bakanlığı desteklidir ve ordu için eleman yetiştirmekten sorumludur.

2015 yılında yapılan bilgi güvenliği araştırmasının sonuçlarına göre İngiltere'de küçük işletmelerin %74'ünün siber güvenlikle ilgili sorun yaşadığı tespit edilmiştir. Bu sonuçtan hareketle ağustos 2015'de internet üzerinden yapılan ticaretin güvenliğini sağlamak amacıyla çevrimiçi çalışan küçük işletmecilere siber güvenlik danışmanlığı ve maddi destek verilmesine karar verilmiştir. E-ticaret sisteminin güvenliğine büyük önem veren İngiltere'nin bu hamlesi, olası tehditler açısından olumlu olarak değerlendirilebilir. Bu noktada İngiltere Hükümeti'nin Ekonomi bakanlığını dijital ekonomi kırılımında ayrıştırmış olması da belirtilmesi gereken bir durumdur.

İngiltere'nin siber güvenlikteki güncel sorunu diğer pek çok ülkedeki gibi siber güvenlik uzmanı eksikliğidir. "ISC'ye bağlı Global Bilgi Güvenliği İşgücü Araştırması'nın son bulgularına göre İngiliz şirketlerinin yüzde 62'sinde çok az

siber güvenlik çalışanı bulunuyor…"[45] Bahsedilen araştırmada, 2020 yılında bilgi güvenliği alanındaki uzman açığı tüm dünyada 1,5 milyona ulaşacağı tahmin edilmektedir. İngiltere, siber güvenlik uzmanı açığı nedeniyle, hüküm giymiş hackerların devlet kurumlarında işe alınmasına imkân sağlayan bir düzenleme yapmıştır. Eylül 2015'den itibaren de bilişim sistemleri alanında lisans seviyesinde eğitim veren tüm bölümlerde, siber güvenlik konusunda eğitim verilmesine karar verilmiştir. Bu şekilde, siber güvenlik alanının sadece bir uzmanlık alanı olması durumunun, her bilişim sistemi mezununun siber bilişim alanlında bilgi sahibi olması şekilde değiştirilmesi hedeflenmektedir. İngiltere, siber suçlarla mücadele amacıyl Siber Güvenlik Operasyonları Merkezi adında, son teknoloji ile donatılmış bir merkez açma hazırlığı içindedir.Savunma Bakanlığı'na bağlı olan ve "teknoloji harikası" siber savunma donanımına sahip olacak bu yeni merkez, savunma altyapısını siber suçlular, hackerlar ve istihbarat nedeniyle sisteme sızmaya çalışan diğer ülkeler gibi kötücül aktörlere karşı savunma görevi yapacaktır.[46]

X. Fransa ve Siber Güvenlik Uygulamaları

Fransa, siber güvenlik alanında iyi bir noktadadır ve oluşturduğu siber güvenlik stratejisini başarı ile uygulamıştır. Söz konusu stratejide dört temel hedef ve yedi aksiyon belirlenmiştir. Bu hedef ve aksiyonlara, önemli örnekler teşkil ettiği için, kısaca değinilecektir. Dört temel hedef şunlardır:

- Siber güvenlikte dünya gücü olmak,
- Fransa bilişim sistemlerinin güvenliğini sağlayarak, Fransa'nın kendi kararını verme özgürlüğünü korumak,
- Kritik sistemlerin siber güvenliğini sağlamak,
- Siber uzayın güvenliğini sağlamak.

[45]"İngiliz üniversiteleri siber savaşçı yetiştirmek için kolları sıvadı" (2015, 4 Temmuz). Erişim tarihi: 15.12.2015. http://siberbulten.org/strateji-guvenlik/ingiliz-universiteleri-siber-savasci-yetistirmek-icin-kollari-sivadi/

[46]"İngiltere siber suçlarla mücadele için son teknoloji üs açmaya hazırlanıyor" (2016, 24 Nisan). Erişim tarihi: 30.04.2016. https://siberbulten.com/strateji-guvenlik/ingiltere-siber-suclarla-mucadele-icin-son-teknoloji-us-acmaya-hazirlaniyor/

Fransa siber güvenlikte dünya gücü olmayı hedeflerken, siber uzayın tek bir hâkimi olmayacağının farkında olarak, tam kontrolün sağlanması için ülkeler arası işbirliğinin önemine vurgu yapmaktadır. Siber güvenlikte dışa bağımlılığın en aza indirilmesinin hayati olması nedeniyle, güvenlik teknolojilerinin geliştirilmesi ve yeni siber güvenlik uzmanlarının yetiştirilmesinin sağlanması hedeflenmektedir. Ayrıca kişisel verilerin korunmasının sağlanması amacıyla Genel Güvenlik Konsepti (The General Security Framework) yayımlanmıştır. Halkın siber güvenlik konusunda farkındalık sahibi olması için çalışılması ve siber uzay güvenliği için hukuki adımların atılması hedeflenmiştir.

Siber güvenlik stratejisinde yer alan yedi aksiyon da aşağıdaki gibidir:

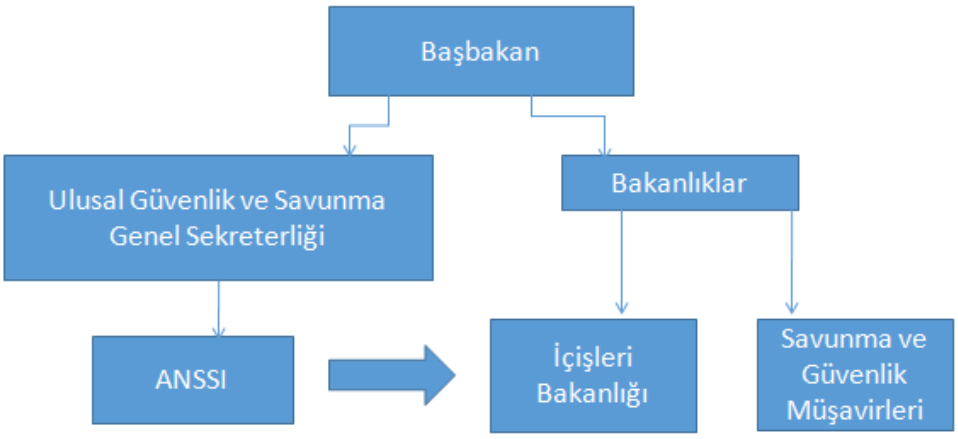
1. Öngör ve analiz et
    - Siber uzayda gelebilecek tehditlerin önceden öngörülmesi ve olası senaryoların analiz edilmesi gerekmektedir.
2. Tespit et, ikaz et, karşılık ver
    - Hem ülkedeki kurumların zayıf noktalarını tespit edilip, kurumların uyarılması hem de saldırı tespit sistemleri ile olası saldırıların tespitinin sağlanması gerekmektedir. Bununla birlikte, olası siber saldırıda ülke sistemleri anında karşılık verecek seviyede olmalıdır.
3. Bilimsel, teknik, endüstriyel ve insan gücünü güçlendir
    - Kamu ve özel sektörün ortaklaşa bir siber teknoloji merkezi kurması ve bilimsel ve teknik anlamda eksiklerin giderilmesi hedeflenmektedir. Genç nüfusun siber güvenlik alanına yönelmesi için çalışmalar yapılmalıdır.
4. Devlet kurumlarının ve kritik yapıların bilgi sistemlerini koru
    - Fransa'da kullanılan akıllı kart ile kimlik doğrulama vb. sistemlerin korunması sağlanacaktır.
5. Fransız hukukunu siber güvenlik gereklerine göre düzenle

6. Uluslararası işbirliğini artır

7. Bilgilendirmek ve ikna etmek için iletişim kur.[47]

Fransa, 2015 Kasım ayında yaşanan Paris saldırısının ardından, siber güvenlik konusunda yaşanabilecek terör eylemleri konusunda yeni bir farkındalık kazanmıştır ve hükümet siber güvenliğin iç ve dış tehditlere karşı güçlendirilmesi için eylem planı hazırlamıştır.

Fransa'da bilgi güvenliği alanındaki politikaları yürütmek amacıyla 2008 yılında Fransız Ulusal Bilgi Güvenliği Ajansı (ANSSI) adlı kurum oluşturulmuştur. Bu kurum direkt başbakanlığa bağlı olan Ulusal Güvenlik ve Savunma Genel Sekreterliği altında yer almaktadır. Kurumun görevi, olası bir saldırı anında harekete geçmek, kurumlar arası koordinasyonu ve saldırı öncesinde kurumların saldırılara hazır hale getirilmesini sağlamak, siber güvenlik alanında ürünlerin geliştirilmesini sağlamak, ağ ve yazılım güvenliği için gerekli donanımları temin etmek hatta geliştirilmesini sağlamak olarak sıralanmaktadır. ANSSI'nın yaptığı çalışmaları ve aldığı kararları uygulayan birimse İç İşleri Bakanlığı'dır. Fransa'nın ayrıca bir CERT Kurumu da bulunmaktadır.



Şekil 4: Fransa'da siber güvenlik uygulamaları organizasyon yapısı[48]

[47]http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf

[48]Orijinal çizim için bknz. Güngör, Murat. "Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma" (2015, Mart)

3. Türkiye'nin Mevcut Durumu

Birçok devlet, siber güvenlik politikaları oluşturmakta, bu amaçla strateji çalışmaları yapmakta ve hedefler belirlemektedir ve bu ülkelerin içinde hatırı sayılır bir kısmı, siber güvenlik politikası geliştirmeye sadece savunma yapmak olarak değil; saldırı yeteneklerini de geliştirmek olarak bakmaktadır. Bu da gelecekte yaşanacak savaşların topla tüfekle değil; internet üzerinden yaşanacağı anlamına gelmektedir. Siber bir silahın, bir ülkenin tüm altyapısını çökertebileceği düşünülürse, siber güvenlik alanında ciddi bir çalışma yapılması gerektiği açıkça görülmektedir. Çünkü gelinen noktada, siber savunma yeteneği olmayan ve sistemleri güvenli olmayan bir ülkenin gizli bilgilerinden de söz edilememektedir.

Türkiye'nin 2013-2014 Eylem Planı Belgesi ve 2016-2019 Siber Güvenlik Strateji Belgesi bulunmaktadır. Bununla birlikte olası bir saldırı durumunda saldırıya uğrayan kuruma destek olmak ve müdahaleyi koordine etmekten sorumlu Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve elektronik haberleşme hizmeti sunan firmaların kendi içlerinde kurdukları Siber Olaylara Müdahale Ekipleri (SOME) bulunmaktadır. USOM, zararlı yazılım analizi yapma, trafik takibi, zararlı yazılım ihbarı alma, kamuoyunu bilgilendirme ve kamu kurumları ve özel kurumlar ile işbirliği sağlama gibi sorumluluklara sahiptir. Bugüne kadar birçok kurumun katılımı ile siber tatbikatlar yapılmıştır. Örneğin 2012 yılında BTK liderliğinde gerçekleştirilen Siber Kalkan Tatbikatı'nda siber saldırıların bertaraf edilebilmesi için teknik yönlerin geliştirilmesi amaçlanmıştır. Ne var ki bu tatbikatların devamı gelmemiş 3 yıldır hiçbir tatbikat yapılmamıştır.

Türkiye'de kamu kurumları, kendisini siber saldırılara karşı hazırlamak konusunda çok yavaş ilerlemektedir. Kamu kurumlarında, siber güvenlik konusunda yetişmiş eleman konusunda sıkıntı yaşanmaktadır. Bu nedenle hem 2013-2014 Eylem Planı maddelerinden hem de 2016-2019 Siber Güvenlik Strateji Belgesi maddelerinden biri, üniversitelerde siber güvenlik eğitiminin yaygınlaştırılması olmuştur. Bu kapsamda bazı üniversitelerde siber güvenlik, bilişim hukuku alanında bölümler açılmıştır ve hali hazırda eğitim vermektedir. Ayrıca TÜBİTAK içerisindeki birimlerden biri olan BİLGEM, siber güvenlik alanında araştırmalar sürdürmektedir. Siber güvenlik alanında çalışmalar yürüten bakanlıkların müsteşarlarından oluşan Siber Güvenlik Kurulu ve özel sektör ile BKT ve TİB kurumlarından uzmanların oluşturduğu Siber Güvenlik İnsiyatifi

grupları bulunmaktadır. Türkiye'nin diğer ükelere göre siber güvenlik uygulamalarındaki yerini gösteren Tablo 1'de görüldüğü gibi, ülkemiz, bu güne kadar siber güvenlik konusuna mesai harcamış ve bu alanda kaynaklara sahip olan ancak gelişmesi gereken bir ülkedir.

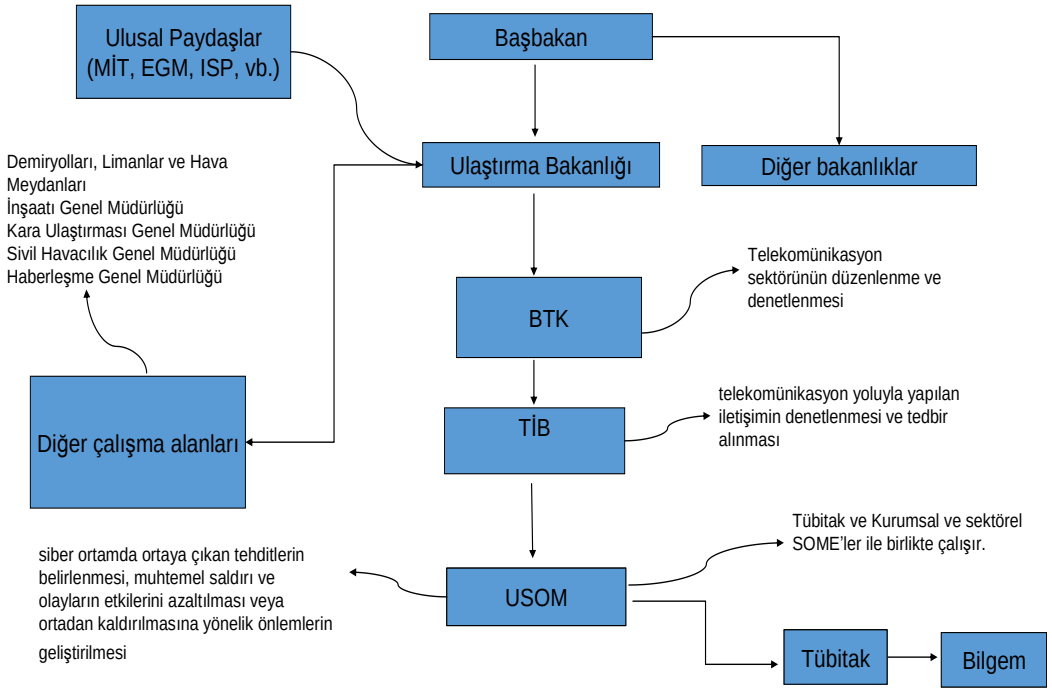
GRUP	ÜLKELER	ÖZELLİKLERİ
Birinci Grup	ABD, Çin, Rusya	Siber güvenlik ve savunma geliştirme çabaları üzerine uluslararası politika koyma kabiliyetine sahip ülkeler. Siber savunma konusunda en büyük desteği veriyor. Siber güvenlik politikaları ve savunma çabalarına en fazla kaynak ve insan desteği sağlıyor.
İkinci Grup	İngiltere, Fransa, İsrail	Birinci gruptaki ülkeleri yakından takip ediyorlar. Ancak daha az personel ve daha kısıtlı altyapıya sahipler.
Üçüncü Grup	Türkiye, Hindistan, Güney Kore, Almanya, Güney Kore	Siber güvenlik politikası ve savunma kabiliyetleri geliştirilmesi için önemli ölçüde kaynak tahsis edilen ülkeler. Ancak bu alanda lider ülke değiller. Birçok durumda, birinci gruptaki ülkeleri takip ediyorlar.
Dördüncü Grup	İsveç, Japonya, Avustralya, Hollanda, İran, Pakistan, Finlandiya	Siber güvenlik ve savunma kabiliyetlerine yönelik kısıtlı kaynak tahsis edilen ülkeler.

Tablo 2:Ülkelerin siber savaş kabiliyetlerinin sınıflandırılması[49]

[49]Orijinal çizim için bknz. Davulcu, Buket. "Sanal dünyada gerçek savaş: Siber saldırılar"(2014, 6 Ocak). Erişim tarihi: 18.12.2015. http://www.aksiyon.com.tr/kapak/sanal-dunyada-gercek-savas-siber-saldirilar_537462

I. Türkiye kurumlarına bakış

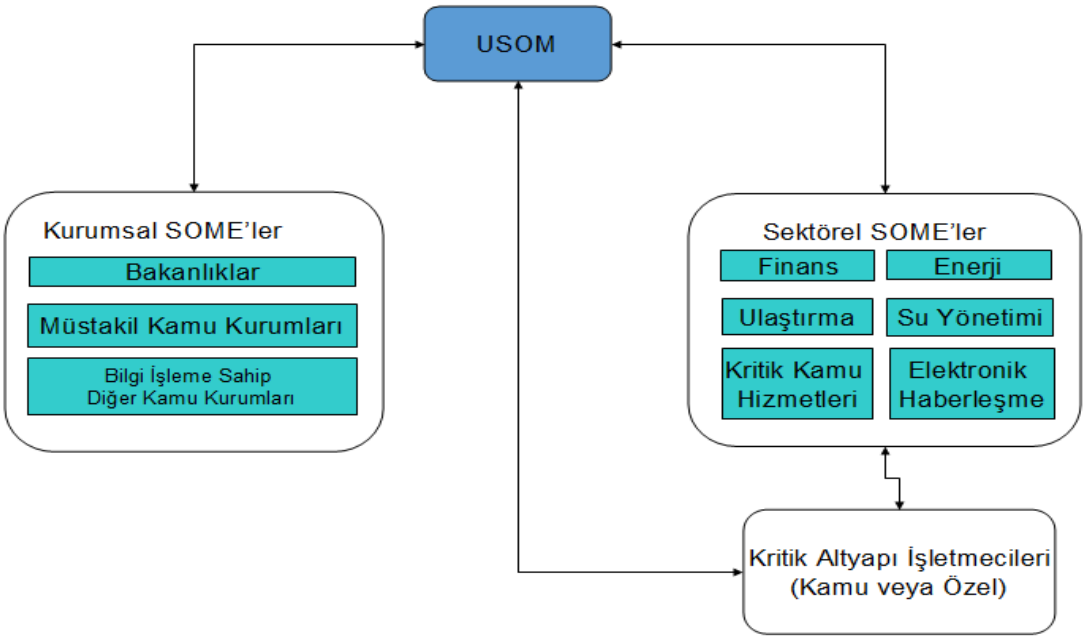
Türkiye'nin mevcutta siber güvenlik uygulamaları yürüten ve siber savunma ile görevli kurumları şekil 5'te görülmektedir. Ülkemizde siber güvenlik konusunda çalışma yürüten kurumların tek çalışma alanı, siber güvenlik uygulamaları ve siber savunma değildir. 2013 yılında kurulan ve siber savunma görevini üstlenen USOM, Telekomünikasyon İletişim Başkanlığı kurumu altında faaliyet gösteren kurumlardan biridir. TİB, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi amacıyla; BTK ise telekomünikasyon sektörünün düzenlenmesi ve denetlenmesi amacıyla Ulaştırma, Denizcilik ve Haberleşme Bakanlığı altında faaliyet göstermektedir. UDHB'nın çalışma konuları, demiryolları, limanlar, hava meydanları, kara ulaşımı, sivil havacılık vb. olarak sıralanmaktadır. Siber güvenlik çalımaları, bu bakanlığın çalışma konularından sadece biridir. Oysa gelinen noktada siber güvenlik, başlı başına bir çalışma alanı olmalıdır. Bir bakanlık altındaki faaliyetlerden biri olması, siber güvenlik konusunda verilen ağırlığın azalmasına neden olmaktadır.



Şekil 5: Türkiye'de Siber Savunma Alanında Çalışan Kurumlar

Siber güvenlik alanındaki teknik uygulamaları gerçekleştiren ve olası bir saldırıda müdahale etmek amacıyla kendini geliştiren USOM'un diğer bakanlıklar

ve SOME'ler ile iletişimi şekil 6'da ifade edimektedir. USOM, siber güvenlik konusunda yazılım geliştirme ve teknik destek sağlama, zararlı yazılım analizi yapma, siber ihbarları toplama ve analiz etme, kurumlar arası koordinasyonu sağlama ve uluslararası kurumlar ile iletişim kurma görevlerini, ayrıca kurumsal ve sektörel SOME'ler ve kritik altyapı işletmecileri ile iletişim kurmak, bir saldırı anında koordinasyon ve teknik destek sağlamak görevini üstlenmektedir. Mevcut durum itibariyle toplam 245 kurumsal ve sektörel SOME kurularak USOM ile irtibatlandırılmış durumdadır. SOME'lerde yaklaşık 720 personel siber güvenlik ile ilgili çalışmalarını sürdürmektedir.[50] USOM, teknik çalışmalarını TÜBİTAK kurumunun siber güvenlik alanında çalışan gruplarından destek alarak ilerletmektedir.



Şekil 6: Türkiye mevcut Siber güvenlik uygulama organizasyon yapısı[51]

II. Tübitak ve siber güvenlik çalışma grupları

Tübitak'ta siber güvenlik alanında çalışma yürüten çeşitli ekipler yer almaktadır. USOM'a bu konuda destek veren en önemli ekip, Bilgem ekibidir. Bilgem, altında

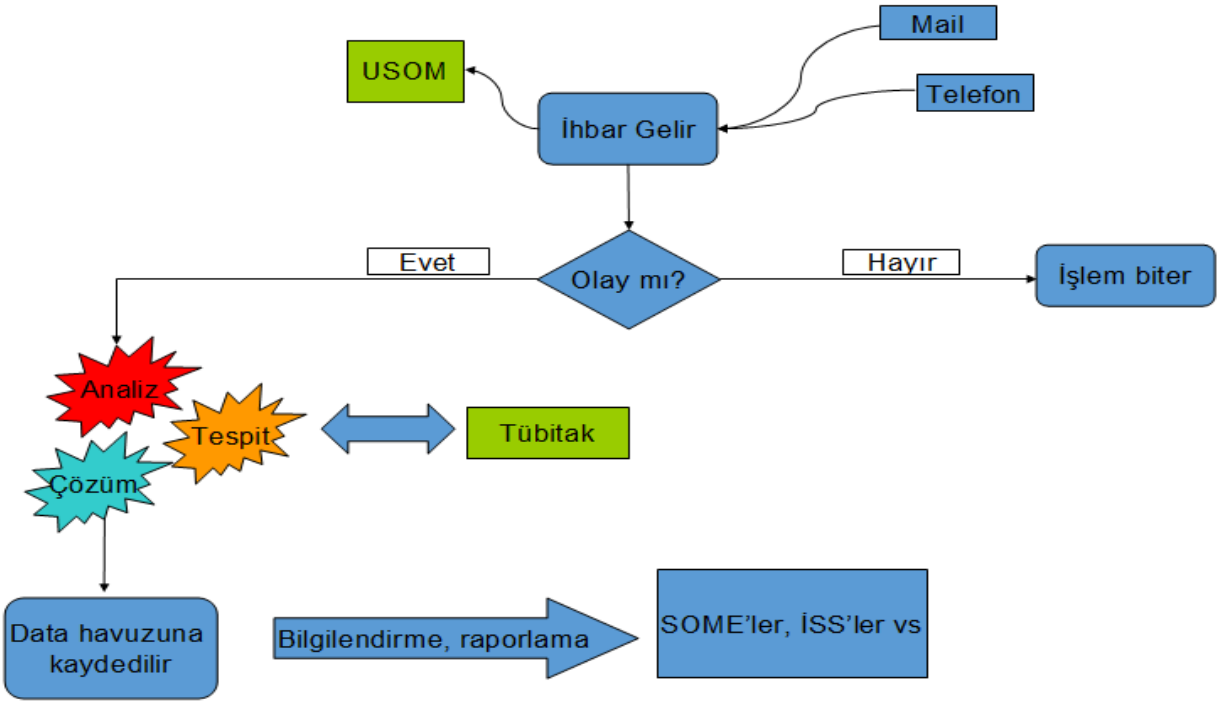
[50]USOM, USOM Faaliyetleri. Erişim tarihi: 04.04.2016. https://www.usom.gov.tr/faydali-dokuman/15.html

[51]Orijinal çizim için bknz. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. "Sektörel SOME Kurulum ve Yönetim Rehberi" (2014 Kasim)

bulunan Siber Güvenlik Enstitüsü'nde bu alanda çalışmalar yürütmektedir. Ancak bu enstitü son zamanlarda aktif değildir.

Tübitak altında siber güvenlik çalışmalarına destek veren diğer kurumlar, bulut bilişim ve Büyük Veri araştırma laboratuvarı, kripto analiz laboratuvarı, tempest laboratuvarı'dır.

USOM, SOME'ler ve Tübitak ile iletişim kurulabilecek ayrıca olay ihbarlarının alınıp değerlendirilebileceği bir platform kullanmaktadır. SOME İletişim Platformu (SİP) adı verilen bu platformun çalışma şekli aşağıdaki gibi özetlenmektedir.



Şekil 7: SOME İletişim Platformu (SİP)İletişim Şeması[52]

USOM, çeşitli kanallar ile siber saldırı istihbaratını almakta ve öncelikle kayda değer olma durumunu değerlendirmektedir. Kayda değer durumlarda, Tübitak gibi paydaşları ile ortak çalışarak saldırıyı bertaraf etmeyi amaçlamaktadır. Bundan sonra, olayı analiz etme, çözümü değerlendirme ve SOME'leri bilgilendirme adımı yer almaktadır. Siber saldırıya uğrayan kurum tarafından ihbar gelmesi süreci ise kurumun kendi SOME'si varsa olaya müdahale etmesi,

[52]Orijinal çizim için bknz. USOM, USOM Faaliyetleri. Erişim tarihi: 04.04.2016. https://www.usom.gov.tr/faydali-dokuman/15.html

gerekirse sektörel SOME ile iletişime geçmesi, bu kurum da çözümsüz kalırsa USOM'a iletilmesi şeklinde ilerlemektedir.

III. Kişisel Verilerin Korunması Kanunu

Uzun yıllardır tasarı halinde bekleyen Kişisel Verilerin Korunması Kanun tasarısı, 24 Mart 2016 tarihinde TBMM tarafından onaylanmıştır. Alınan karara göre, 8., 9., 11., 13., 14., 15., 16., 17. ve 18. maddelerin yayım tarihinden altı ay sonra yürürlüğe girmesi beklenmektedir. Bu maddeler dışındaki maddeler ise kanun onaylandıktan hemen sonra yürürlüğe girmiştir.

Kanun ile birlikte hayatımıza giren hususlar kısaca aşağıdaki gibidir:

- Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, özel nitelikli kişisel veri sayılacak.
- Kişisel veriler ve özel nitelikli kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemeyecek.
- Aydınlatma yükümlülüğü kapsamında kurumlar, veri toplamadan önce ilgili kişiye, kişisel verilerinin hangi amaçla toplanacağı ve işleneceği, hangi taraflarla paylaşılacağı gibi hususlar hakkında bilgi verecek,
- Veri toplayan kurumlar, kişisel verilerin güvenliğini sağlayacak önlemler alacak,
- İşlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler silinecek, yok edilecek veya anonim hale getirilecek.
- Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamayacak.
- Sadece bu konularla ilgili düzenleme ve yönetim için Kişisel Verileri Koruma Kurumu adı altında yeni bir otorite oluşturulacak.
- Bu kanuna uygunsuz davranan kurumlara idari ve/veya adli cezalar uygulanacak.

Ülkemizin bir kişisel verilerin korunması kanununun olmaması, uluslararası arenada Türkiye'yi zor durumda bırakmakta idi. Bu kanunun çıkması ve bahsedilen Kişisel Verileri Koruma Kurumu'un en kısa sürede kurularak faaliyete geçmesi, siber güvenlik alanında diğer ülkeler ile yapılacak ortak çalışmaların önünü açacaktır. Birçok ülke, kişisel verilerin korunması

konusunda bir çalışma olmadığı için, Türkiye ile bilgi paylaşımına sıcak bakmamakta idi.

IV. 2016-2019 Siber Savunma Strateji Belgesi

Türkiye ilk siber savunma stratejisini 2013 yılında oluşturmuş ve burada alınan kararların bir kısmını ciddi anlamda uygulamıştır. Ancak bu strateji ve uygulamalar, çok büyük hızla ilerleyen teknoloji ve bu nedenle açılan yeni sanal cephelere yetişmek için yeterli değildir. Nitekim, okumakta olduğunuz tezin yazılmakta olduğu günlerde, Türkiye çok ciddi bir siber saldırıya maruz kalmıştır. Yapılan Ddos ataklarına karşı çok büyük etkinlik gösterilememiş ve bu sayede ülkemizin siber güvenlik ve siber savaş alanındaki eksikliği bir anlamda gün yüzüne çıkmıştır. Bu saldırıları izleyen günlerde, 2016-2019 Siber Savunma Strateji Belgesi çalışmaları tamamlanmıştır. Bu belgenin oluşturulması ve 2019 yılına kadar siber alandaki hedeflerin belirlenmesi önemli bir adımdır.

Yeni siber savunma stratejisinin kararları ve hedefleri şunlardır:

- Ulusal kritik altyapı envanterinin oluşturulması, kritik altyapıların güvenlik gereksinimlerinin karşılanması ve bu kritik altyapıların bağlı oldukları düzenleyici kurumlar tarafından denetlenmesi.
- Siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması.
- Sektör düzenleyici kurum, bakanlık vb. kuruluşların siber güvenlik kapsamında düzenleme ve denetleme farkındalıklarının ve yetkinliklerinin geliştirilmesi.
- Kurumların bilişim sistemlerinin sadece saldırılardan değil, kullanıcı hataları ve afetlerden de korunması için düzenlemelerin yapılması.
- Her kurumun kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe ulaşması.

- Siber güvenlik konusunda kurum yöneticilerinin farkındalığının artırılması.

- Siber güvenlik alanında yetkin personel yetiştirilmesi ve bu alanda uzmanlaşmak isteyen personel, araştırmacı ve öğrencilerin teşvik edilmesi,

- Toplumun her kesiminde siber güvenlik bilincinin oluşturulması, eğitim kurumlarının çalışmalarına ilave olarak yazılı ve görsel medyada farkındalık çalışmalarının yapılması.

- Kamu kurumlarında siber güvenlik alanında uzman personel istihdam edilmesi için mevzuat desteği sağlanması ve personelin özlük haklarının iyileştirilmesi.

- Kurumsal ve Sektörel SOME'lerin (Siber Olaylara Müdahale Ekibi) etkinliğinin arttırılması için mevzuat desteğinin sağlanması, mali düzenlemelerin yapılması, yetkin personel ihtiyacının karşılanması, bilişim altyapısının sağlanması ve ulusal siber olaylara müdahale organizasyonu kapsamında bilgi paylaşımının geliştirilmesi.

- Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması.

- Kamu kurumları, özel sektör, STK'lar (Sivil Toplum Kuruluşu), denetleyici kurumlar, üniversiteler, geliştirici firmalar ve tüm diğer paydaşların katılım ve koordinasyon hedefi ile ulusal siber güvenlik eko-sisteminin oluşturulması.

- Ulusal Siber güvenlik eko-sistemi içinde iyi örneklerin yaygınlaştırılması, danışmanlık hizmetlerinin verilmesi, açıklık, tehdit ve faydalı uygulamaların paylaşılması.

- Bilişim sistemlerinin kritik noktalarında kullanılan, yerli veya yabancı donanım ve yazılım ürünlerinin içerdiği açıklıkların kötüye kullanılmasına engel olmak üzere açıklık analizi ve sertifikasyon çalışmalarının yapılması.

- Güvenli yazılım geliştirme ve tedarik yönetimi kültürünün oluşturulması.

- Siber güvenlikte dışa bağımlılığı azaltmak için Ar-Ge faaliyetlerine önem verilerek yerli ürünlerin geliştirilmesi.

- Tehdit unsurlarının saldırı yapmadan önce bertaraf edilmesi için ulusal proaktif siber savunma yeteneğinin geliştirilmesi.

- Tehdit unsurlarının siber uzaydaki en büyük avantajı olan anonimliği ortadan kaldırmak için etkin kayıt yönetimi ve IPv6 (Internet Protokolü sürüm 6) teknolojilerinin yaygınlaştırılması.

Yeni hazırlanan 2016-2019 Strateji Savunma Belgesi, ülkemizin siber savunma sisteminin güncelliğinin ve devamlılığının sağlanması adına önemli olmuştur. 2013 yıındaki siber savunma belgesine göre çok daha vizyoner olmakla birlikte, belgede eksikler bulunmaktadır.

Belgede siber savunma ile ilgili bir seferberlikten bahsedilmektedir. Siber güvenlik çalışmaları kapsamında üniversitelerle işbirliği yapılması planlanmaktadır ve kritik yapıların güvenliğinin önemine vurgu yapılmaktadır. Diğer yandan siber savunmadan sorumlu bir kamu otoritesinden bahsedilmektedir ancak bu otoritenin nasıl bir konumda olacağı, yetkileri, organizasyondaki yerine dair hiçbir bilgi bulunmamaktadır. Kamu otoritesinin detaylandırılması ve bu amaçla ciddi adımlar atılması gerekmektedir. Ek olarak Belgede siber güvenlik sadece sivil kurumlar için incelenmiştir. Ordunun siber savunmadaki yerine değinilmemiş olması da önemli bir eksiktir.

Türkiye, son birkaç ayda veri koruma kanunun yasalaşması ve 2016-2019 siber savunma belgesinin yayınlanması ile siber savunma alanında çalışmalarını hızlandırmıştır. Ayrıca Türkiye, NATO'nun Siber Savunma Mükemmeliyet Merkezi'ne (CCD COE) sponsor üye olmuştur. Tüm bu çalışmalar, Türkiye'nin siber güvenlik alanında, uluslararası arenada görünür olabilmek ve söz sahibi olmak adına atılmış adımlar olarak değerlendirilebilir ve çok önemlidir.

4. Türkiye Modeli Önerisi

Türkiye, siber güvenlik konusunda kötü bir konumda olmasa da sahip olduğu potansiyele göre değerlendirildiğinde, olması gerektiği noktada bulunmayan bir ülkedir. Bu çalışmanın yapıldığı dönemde meydana gelen ve Türkiye'ye yönelik DDoS atakları ile yaşanan tr uzantılı sitelere erişilememesi, bankacılık sistemlerinin işlem yapamaz hale gelmesi gibi olaylar, ülkemizin siber güvenlik alanındaki konumuna dair öz eleştiri yapılması ve eksikliklerin giderilmesi için büyük bir fırsat olarak görülmelidir. Nitekim tablo 3'te görüldüğü gibi, bugün siber güvenlik alanında gelişmiş olan ülkelerin hepsi, sıkça siber saldırıya uğrayan ülkelerdir.

	Siber güvenlik stratejisi	Ulusal CERT	Diğer CERT	Siber Tatbikat	Siber Komutanlık	EGC FIRST	Kurum
ABD	X	X	X	X	X	FIRST	USCYBERCOM/NSA
Almanya	X	X	X	X	-	EGC	-
Avustralya	3X	X		X	-		Cyber-Security Operations Centre
Avusturya	3x Taslak	X	X	-	-	-	-
Brezilya	X		X		X		Information Security Department
Çin	X	X	X	X	*		*
Danimarka	-	X	X		-	EGC	-
Estonya	X	X	X	X	-	EGC	CCDCOE (NATO)
Finlandiya	-	X		X	-		-
Fransa	X	X	X	X	-		-
Hindistan	Taslak	X	X	X	X		Cyber Command and Control Authority.
Hollanda	X	X	X	X	-	EGC	-
İngiltere	X	X	X	X			Cyber-security Operations Centre
İspanya	-	X	X	X	-	EGC	The National Intelligence Service
İsrail	X	X	X		X		*
İsveç	X	X	X	X		EGC	-
İtalya	-	X	-	X	-	-	National Computer Crime Centre for Critical Infrastructure Protection
Japonya	X	X	X	X	-	*JPCERT/CC FIRST*	National Information Security Centre
Kanada	X	X	X		-	-	-
Polonya	-	X	X	X	-	-	-
Romanya	X	X	X	X	-	-	-
Rusya	X	X	X		*	FIRST	-

Tablo 3: Ülkelerin siber güvenlik alanındaki durumları[53]

[53]Bakır, Emre. "5. Boyutta Savaş: Siber Savaşlar – II" (2012, 2 Ocak). Erişim tarihi:21.12.2015. https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-ii.html

Siber saldırılarda, zombi bilgisayarlar kullanılması nedeniyle saldırganın kimliğinin çoğu zaman saptanamaması; saldırganların bir sistemin tek bir açığına yoğunlaşmasına karşılık, sistemin korunması için sistemde tüm açık olma ihtimali bulunan kısımların tespit edilmesinin gerekmesi nedeniyle saldırganlarla mücadelenin zor bir süreç olması gibi sebepler, siber uzayda saldırganlara yapılan mücadelede göz korkutmamalıdır. Çünkü, saldırganların çoğu zaman ülkelerden veya şirketlerden bir adım önde olması, teknik anlamda gelişmeyi de beraberinde getirmektedir.

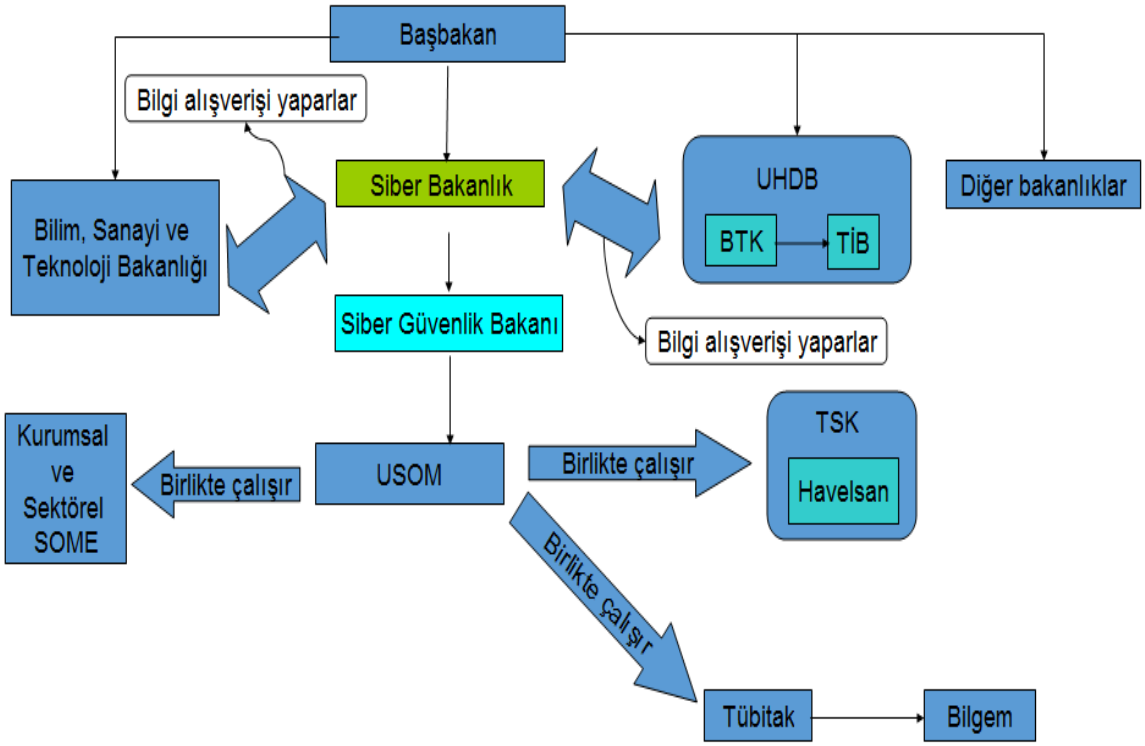
I. Kamu Kurumlarının Yapılandırılması

Siber güvenlik uygulamaları incelenen ülkelerden bu alanda en iyi durumda olan ABD'nin en dikkat çekici yönü, siber güvenlik alanında çalışma yapan teknik kişilerin herhangi bir bakanlık vb. bir yapıya değil; "Chief of Staff" denen bir siber bilişim şefine bağlı olması ve bu şefin de direkt başkan Barrack Obama'ya bağlı olmasıdır. Şef, altında çalışan siber bilişim ekiplerinin hepsini koordine eder ve acil durumlarda başkana hızlı bir şekilde bilgi iletebilir. Bu da çok hızlı harekete geçmeyi sağlar. Türkiye'de siber güvenlik alanındaki çalışmalar, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı çatısı altında yürütülmektedir. Bu şekilde yürütülmesi, birçok aksaklığa neden olmaktadır. Çünkü siber güvenlik, günümüzde her ülke için en önemli odak noktalarından biri haline gelmiştir ve bir bakanlığın çalışma alanlarından biri olması değil; tek başına bir sorumluluk alanı ifade etmesi gerekmektedir. Ayrıca siber güvenlik alanında çalışma yürütecek kurumun hangisi olduğu ve karar alacak kurumun yetkileri kesin çizgilerle belirlenmediği için karışıklık ortaya çıkmaktadır. Bu da hem bir saldırı durumunda hızlı aksiyon almayı engellemekte hem de siber güvenlik alanındaki ilerlemenin ivmesini düşürmektedir. Önerilen Türkiye Modeli'nde, siber güvenlik alanındaki çalışmaların yönetiminden, direkt Başbakan'a bağlı bir siber güvenlik bakanının sorumlu olması gerektiği öngörülmektedir. Böylece hem olası bir saldırı durumunda hızlı aksiyon alınabilecek hem de tüm siber güvenlik birimlerinin yönetilmesi ve koordinasyonu kolaylaşacaktır. Birimlerin görev ve sorumluluklarının kesin çizgilerle ayrılması, kriz sırasındaki müdahalenin yönetilmesini kolaylaştıracaktır.

Türkiye'nin 2016-2019 yılı için hedeflerinin belirlendiği Ulusal Siber Güvenlik Stratejisi Belgesi'nde "Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması." şeklinde siber güvenlik alanında yönetimin tek bir merkezde toplanması konusuna değinilmektedir. Ancak bu konu detaylandırılmamıştır. Bu çalışma kapsamında siber güvenlik ve siber savunmanın başlıbaşına bir alan haline gelmiş olmasından dolayı, kabine altındaki yeni bir bakanlık olarak konumlandırılması önerilmektedir. Şekil 8'de ifade edildiği gibi, siber güvenlik bakanı atanması ve bu alanda faaliyet gösteren kurumların da bu bakanlığa bağlı olması, böylelikle siber güvenlik konusunun bir bakanlığın çalışma alanların biri olmak yerine başlı başına bir alan olması öngörülmektedir. Ayrıca siber güvenlik alanının bir bakanlığın çalışma alanı içinde olması, olası bir siber saldırı veya savaş durumunda hızlı aksiyon alınması açısından elzemdir. Türkiye'nin mevcut siber güvenlik işleyişinde bu alanda çalışan birimlerin UHDB altında konumlandırılması, sistemin işleyişini yavaşlatmaktadır.

Yeni siber güvenlik siteminde USOM'un, siber güvenlik bakanına direkt bağlı olması önerilmektedir. USOM'un şu andaki işleyişteki gibi SOME'ler ile koordinasyon halinde olması, teknik desteği Tübitak'tan alması durumunun korunması ancak BTK ve TİB'ile telekomünikasyon ile ilgili konularda destek almak ve destek vermek misyonun üstlenmesi önerilmektedir. Ayrıca mevcutta TSK altında çalışmalarını sürdüren ve siber güvenlik, kritolama gibi alanlarda başarılı çalışmalar yürüten Havelsan'ın da siber savunma organizasyonuna dahil olması önerilmektedir. Siber güvenlik bakanlığı altında, hem teknik hem de hukuki konularda çalışan birimler kurulmalıdır. Bu birimlerin sıfırdan kurulması söz konusu değildir. Mevcutta TİB altında siber güvenlik çalışmaları yapan ekiplerin, siber güvenlik bakanlığı altında çalışmalarına devam etmesi ayrıca yeni bakanlık altındaki kurumların da sektör bazında ayrıştırılması önerilmektedir. Yeni kurulacak Siber Bakanlık altında bulunması önerilen birimler şunlardır: Siber Güvenlik Eğitim Dairesi Başkanlığı, Kurumlar Arası Koordinasyon ve İletişim Başkanlığı, Strateji Geliştirme Başkanlığı, Kritik Yapı Güvenliğinden Sorumlu Başkanlık (sektör kırılımında), USOM, Hukuk Müşavirliği, TeknolojiTakip ve Geliştirme Başkanlığı. Ayrıca Bilim, Sanayi ve Teknoloji Bakanlığı altında konumlandırılmış olan Bilim ve Teknoloji Genel

Müdürlüğü ile de yeni projelerin geliştirilmesi, mevzuatların oluşturulması, toplumun siber güvenlik konusunda eğitilmesi ve farkındalık edinmeleri konusundaki çalışmalarda birlikte hareket edilmesi gerektiği düşünülmektedir.



Şekil 8: Önerilen siber güvenlik ortamı organizasyon yapısı

II. Mevcut USOM ve SOME Yapısının Geliştirilmesi

Türkiye'de hali hazırda yer alan USOM (Ulusal Siber Olaylara Müdahale Merkezi), bahsedilen yapıya uyarlanmalıdır. USOM, altında yer alan kurumsal SOME'ler geliştirilmelidir.Ayrıca sektörel SOME'ler geliştirilmeli, sayıları artırılmalı ve USOM ile koordinasyonu kuvvetlendirilmelidir. Kritik sistemlerin siber saldırılardan korunması en önemli ve dikkatle incelenmesi gereken kısımlardan biridir. Bu sistemlerin kamu veya özel sektöre tarafından yönetiliyor olmasına göre, her birinin ayrı SOME yapısı oluşturulması sağlanmalı ve teşvik edilmelidir.

III. Ulusal CERT Kurumunun Geliştirilmesi

Mevcutta bulunan ulusal CERT Kurumu, USOM altında çalışma yürütecek şekilde yapılandırılmalı ve yetenekleri geliştirilmelidir. Bu kurumun görevleri aşağıdaki gibi sıralanabilir:

- Bütün bilgisayar ve ağ sistemlerini, hükümet sistemlerini korumak,
- Ülke genelindeki kamu ve özel tüm kurumlara ve sistemlere ait risk analizi yapmak ve sonuçları kurumlarla paylaşmak,
- Siber güvenliğe dair yeni tekniklerin takibinin sağlanması,
- Teknolojinin gelişimi ile ortaya çıkan uygulamaların (Örneğin; mobil cihazların güvenliği, bulut bilişim, kablosuz iletişim) güvenliği üzerine çalışmaların yürütülmesi,
- Yeni yöntemlerin ve tekniklerin hem kamu hem de özel sektör kurumları ile paylaşılması,
- Diğer ülkelerin CERT kurumları ile güçlü bağlantılara sahip olunması ve gerektiğinde birlikte çalışmanın koordinasyonu,
- Erken uyarı sisteminin oluşturulması, geliştirilmesi, güncelliğinin sağlanması,
- Erken uyarı sisteminin 7/24 prensibine göre takip edilmesi ve olası saldırı durumunda saldırıya uğran kurum veya kurumların SOME'lerine bilgi verilmesi ve müdahalenin sağlanması,
- SOME kurumlarının çalışanlarının ve kendi çalışanlarının eğitiminin organize etmek ve sertifikalandırma sağlamak,
- Ülke genelindeki siber güvenlik potansiyelini tespit etmek, ilgisi olan kişilerin başvurularını almak ve değerlendirmek,
- US-CERT yapısında olduğu gibi internet aracılığı ile ihbar almak. İhbarları "yazılım açığı" ve "siber saldırı/siber olay" olarak ayırmak ve müdahalede bulunmak,
- Yeni siber bilişim uzmanlarını ve uzman adaylarını keşfetmek,

- Üniversiteler ve akademisyenler ile iletişim halinde olmak.

IV. Mevcut Siber Güvenlik Kurulu'nun Geliştirilmesi

2012 yılında kurulan Siber Güvenlik Kurulu, çalışmalarını Ulaştırma, Denizcilik ve Haberleşme Bakanlığı başkanlığında yürütmektedir. Bu kurulu, Dış İşleri, İç İşleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme Bakanlıkları'nın müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muharebe Elektronik Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurulu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Kurumu Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanı tarafından belirlenecek, bakanlık ve kamu kurumlarının üst düzey yöneticileri oluşturmaktadır.[54]

Kurulun görevleri şu şekilde sıralanabilir:

- Siber güvenlik alanındaki politikaları, stratejileri ve eylem planlarını onaylamak, ülke çapında etkin olarak uygulanması için gerekli kararları almak,

- Kritik altyapıları belirlemek,

- Siber güvenlikle ilgili kararların tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşların belirlenmesi,

- Kanunlarla verilen diğer görevleri yapmak.

Bu kurul, ilk toplantısında USOM'un kurulması kararını almıştır ve bu karar 15 Mayıs 2013 tarihinde hayata geçirilmiştir.

Geliştirilecek sistemde, bu kurulun Ulaştırma, Denizcilik ve Haberleşme Bakanlığı başkanlığında değil; Siber Güvenlik Bakanı başkanlığında ve USOM çatısı altında yürütülmesi, önerilmektedir. Kurulun üyeliğine seçilecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinin de Siber Güvenlik Bakanı tarafından belirlenmesi, ayrıca üst düzey yöneticilerin sadece kamu kurumlarından değil; özel sektörün gerekli görülen firmalarında da seçilmesi önerilmektedir.

[54]Yıldız, Mithat. "Siber Suçlar ve Kurum Güvenliği" (2014 Kasim)

Böylece kamu-özel sektör ortaklığı sağlanmış ve de özel sektörün deneyimlerinden de faydalanılmış olacaktır. Ayrıca, siber güvenliğin eğitim ayağının önemi düşünüldüğünde, bu kurula Milli Eğitim Bakanlığı Müsteşarı da katılmalıdır. Siber Güvenlik Kurulu'nun Türkiye Siber Güvenlik Stratejisini oluşturması sağlanmalıdır. Ayrıca strateji dinamik olmalı ve gelişen teknoloji ve ihtiyaçlara göre sürekli güncellenmelidir. Siber Güvenlik Kurulu'nun atması gereken en önemli adım ise, son iki yıldır ara verdiği toplantılarına devam etmek olmalıdır.

V. Mevcut Siber Güvenlik İnsiyatifinin Geliştirilmesi

Siber Güvenlik İnisiyatifi, İnternet Geliştirme Kurulu[55] altında toplanan özel sektör temsilcilerinin, siber güvenlik alanında fikir ve görüş alışverişinde bulunmak, yeni fikirler üretmek için çalışmalar yaptığı ve bu fikirleri Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na sunan topluluktur. İnsiyatif'in hedefleri, vatandaşın ve küçük işletmelerin siber güvenlik ve veri güvenliği konusunda bilgilendirilmesi, farkındalık yaratılması, şirketlerin ve ISS'lerin minimum güvenlik seviyesinin belirlenmesi, risk analiz yapma, standartların belirlenmesi, rapor yayınlanması olarak sıralanmaktadır.[56] Siber Güvenlik İnsiyatifi üyeleri arasında Kaspersky Lab, Netaş, Turkcell, TTNET gibi kurumlar yer almaktadır.[57]

Önerilen sistemde bu insiyatifin de raporlarını USOM'a sunması gerekmektedir. Özel sektörün deneyimlerinden faydalanılması için bu topluluğun aktif bir şekilde çalışmasının sağlanması gerekmektedir. Siber Güvenlik Kurulu'na seçilecek özel sektör temsilcilerinin, insiyatif içindeki üyelerden biri olması sistemin birbirini tamamlayan parçalar bütünü haline gelmesini sağlayacaktır. İnsiyatifin, siber güvenlik farkındalığı konusunda ulusal bir kampanya başlatması gerekmektedir. Kampanya iki ayak şeklinde yürütülmeli, vatandaşlar ve kamu/özel sektör çalışanları için bilgi güvenliği, dijital deliller ve siber güvenlik konusunda bilinç oluşturacak çalışmalar yürütülmeli ve bu amaçla kitapçıklar hazırlanmalıdır. Çalışanlara yönelikyürütülen kampanya ve kitapçık ile vatandaşlara yönelik kampanya ve kitapçık farklılaştırılmalıdır. Ayrıca İngiltere

[55]Internet ortamının kullanım şartlarını düzenlemek ve internetin etkin kullanımı amacıyla politika ve strateji önerileri hazırlamak için 2011 yılında kurulan kurul.
[56]Yıldız, Mithat. "Siber Suçlar ve Kurum Güvenliği" (2014 Kasim)
[57]http://www.internetkurulu.org/tr/SGInsiyatifi.aspx

Hükümeti'nin yaptığı gibi küçük işletmelere/kobilere siber güvenlik alanında destek olacak bir proje yürütülmelidir.Örneğin; 2015 yılı Bilgi Güvenliği Araştırması'nın sonuçlarına gore İngiltere'de küçük işletmelerin %74'ü siber tehditlere karşı korunmasız durumdadır.[58]Bu da küçük şirketlerin, siber suçlular için hedef haline gelmesine sebep olmaktadır. Bu nedenle siber güvenlik konusunda devlet kurumlarının küçük şirket sahiplerine danışmanlık yapması, siber güvenlik ve veri güvenliği sistemlerinin tahsisi için belli miktarda maddi destek vermesi önerilmektedir.

VI. Siber Ordu Kavramı

Günümüzde savaşlar, bilindik anlamından sıyrılmıştır ve gelişen teknoloji ile savaş literatürü de değişmeye başlamıştır. Gelinen noktada siber savaşlar daha çok hackerler üzerinden yapılıyor olsa da yakın gelecekte ülkeler arası siber savaşların yaşananılması kaçınılmazdır. Bu duruma ABD'nin, son zamanlarda büyük yankı uyandıran terör saldırıları gerçekleştiren Işid örgütüne siber savaş ilan etmesi örnek gösterilebilir.[59]Daha önceki bölümlerde incelenen ülkelerin birçoğu askeri ordularını siber güvenlik alanında bilgili uzmanlarla donatmıştır. Birçok ülke hem savunma hem de saldırı amaçlı olarak siber alanda hazırlıklar yapmaktadır. Böyle bir ortamda askeri gücün de siber savunma teknikleri konusunda çok iyi noktada olması gerekmektedir. Bu nedenle, Türkiye de ordu içersindeki siber güvenlik departmanının geliştirilmesi ve siber güvenlik konusunda askeriyenin diğer birimlerinden farksız hale getirilmesi için çalışmalarını yürütmelidir. Kara, hava ve deniz olmak üzere 3 gruptan oluşan TSK kuvvet yapısına, "siber uzay" eklenmelidir. Bu konuda İsrail'in UNIT 8200 birimi örnek alınabilir. Ordunun hem siber güvenlik konusunda güçlü bir uzman kadrosu ile donatılması ve siber komandoluk mesleğinin tanımlanması hem de "askeri siber güvenlik" konusunda geleceğin elemanlarını yetiştirmek için eğitim vermesi önerilmektedir. Ayrıca yine İsrail Ordu'sunun uyguladığı bir yöntem olan, zorunlu askerlik döneminde isteyen kişilere siber güvenlik eğitimi verilmesi ve bu şekilde yetenekli gençlerin sisteme kazandırılması Türkiye'de de uygulanabilir. Böylece ciddi bir sorun olan siber güvenlik uzmanı bulmakonusunda bir kaynak daha oluşturulmuş olacaktır. Siber güvenlikte, mihenk taşlarından biri siber

[58]Pwc. "2015 Information Security Breaches Survey" (2015)
[59]https://siberbulten.com/uluslararasi-iliskiler/abd-iside-karsi-siber-savas-ilan-etti/

güvenlik konusunda çalışacak uzmanların yetiştirilmesidir. Bu alanda çalışacak siber güvenlik uzmanlarının (komandolarının) da siber güvenlik bakanına direkt bağlı olmaları sistemin bütünlüğünün sağlanması açısından gerekli görülmektedir. Ek olarak, TSK'ya bağlı olarak çalışma yürütmekte olan Havelsan Kurumu'nun yeteneklerinden faydalanılması gerekmektedir. Yukarıda bahsedilen siber güvenlik alanında yetenekli ve istekli kişlerin sisteme kazandırılması amacı, Havelsan ile ortak geliştirilecek bir proje ile hayata geçirilebilir.

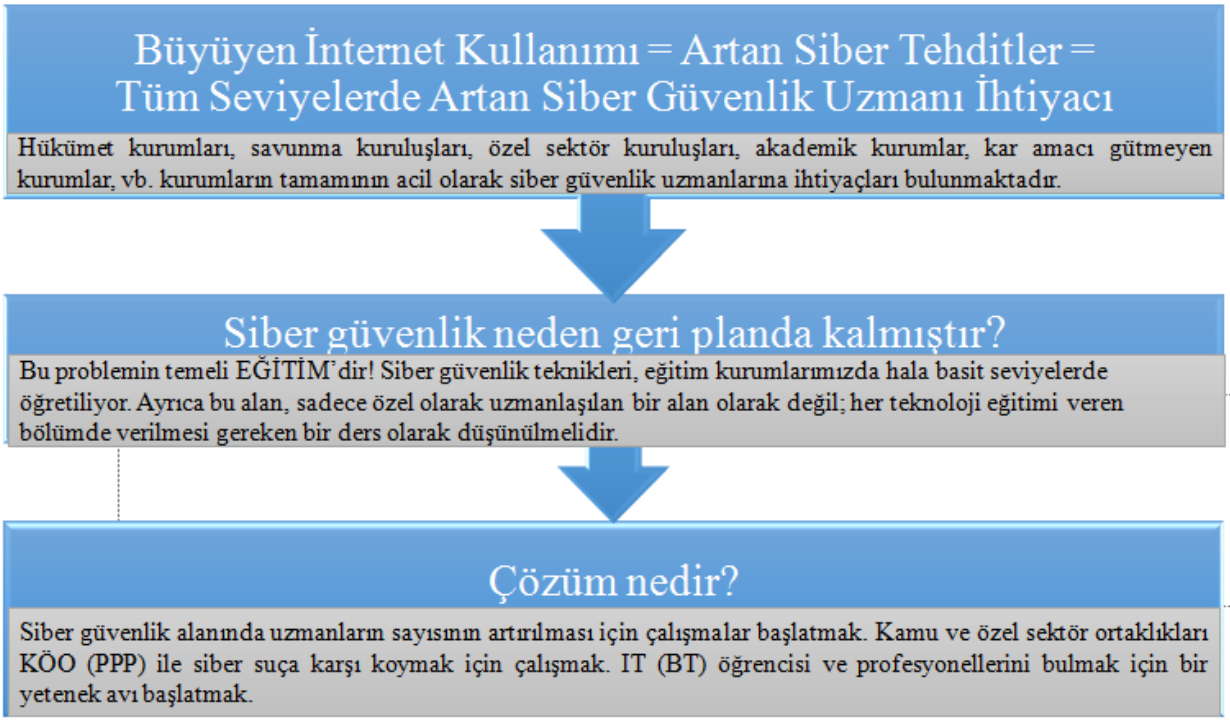
VII.Siber Güvenlik Laboratuvarı Kurulması

Siber güvenlik alanında iyi bir konuma gelmek önemli ancak sadece var olan savunma tekniklerini bilmek değil; bu tekniklerin yerlilerini üretmek ve geliştirmek gerekmektedir. Kullanılan firewall yazılımlarından, erken uyarı sistemlerine, kritik yapıların korunması için kullanılan yazılımlara kadar farklı ülkelerde üretilmiş yazılımları kullanarak siber güvenlik alanında çalışmak, Truva Atı gibi bir sisteme sahip olmak anlamına gelebilmektedir. İçinde ne olduğunu bilmeden bir yazılımı kullanmak, efektif bir yol olmayacaktır. Ayrıca bir sistemin güvenilirliğini, olası bir saldırı durumundaki tepkisini test etmenin en iyi yolu, kendini sisteme sızmaya çalışacak kişinin yerine koyarak test etmektir**.** Bu nedenle Türkiye CERT Kurumu içerisinde bir siber güvenlik laboratuarı kurulması ve ülkenin bilgisayar mühendisliği alanında iyi derecede eğitim vermekte olan okullarının bu bölümlerinde de küçük çaplı siber güvenlik laboratuarlarının kurulması önerilmektedir. Ayrıca siber güvenlik alanında önemli çalışmalar yapmakta olan Havelsan'ın potansiyelinin de bu amaçla kullanılması akıllıca olacaktır.

VIII. Siber Güvenlik Alanında İş Gücünün Temini

Siber güvenlik alanında yapılan tüm araştırmalarda gelecek yıllarda karşılaşılacak en büyük problemin siber güvenlik iş gücü temini olacağı belirtilmektedir. Bu nedenle hem güncel projelerde çalışacak uzmanların bulunması ve eğitimi hem de gelecek neslin siber güvenlik uzmanlarının yetiştirilmesi için şimdiden çalışılmalıdır. Siber güvenlik çalışmaları içerisinde bu konuya da emek verilmeli ve projeler geliştirilmelidir. Hindistan Telekom'un yaptığı bir çalışmada siber güvenlik uzmanı konusundaki Hindistan'ın durumunu özetlediği şekil 9'daki diyagram, ülkemiz için de geçerlidir**.** Gelişen teknoloji ile

hayatımızın her alanına giren akıllı cihazlar, akıllı cihazlar vasıtası ile gündelik hayatın vazgeçilmez bir parçası haline gelen sosyal medya ve sosyal medya vasıtası ile ortalığa saçılan birçok bilgi; ayrıca devlet kurumlarınn işlemleri internet üzerinden yapar hale gelmesi, hayatımıza birçok fayda getirdiği gibi bilginin korunması konusunda da yeni sorunlara sebep olmuştur. Bilginin korunmasının güçleşmesi ve internet üzerinden işlenebilecek suçların çeşitliliği ile teknolojinin her geçen gün daha büyük bir ivme ile ilerlemesinin sonucu olarak siber güvenlik uzmanı ihtiyacının artışı birbirine paralel olacaktır. Bu nedenle dünyadaki birçok ülke gibi, Türkiye'nin de siber güvenlik alanındaki hem güncel uzman açığının kapatılması hem de gelecekteki muhtemel ihtiyaçlara şimdiden hazırlık yapılması için çalışması gerekmektedir.



Şekil 9: Siber güvenlik alanında iş gücü ihtiyacının artışı ve çözümü[60]

Siber güvenlk alanında iş gücünün temin edilmesi için öneriler, aşağıda sıralanmaktadır.

- Meslek liselerinin bilgisayar bölümlerindeki potansiyelin kullanılması önerilmektedir. Meslek liselerinden mezun olan öğrenciler, mevcut sistemde iş

[60] Orjinal çizim için Bknz. Kumar, Mukherjee. "Cyber Security in India: A Skill Devolopment Perspective" (2013)

bulmak ve kendilerini geliştirmek konusunda zorlanmaktadır. Bu öğrencilerin potansiyelinin kaybedilmemesi için, geleceğin siber güvenlik uzmanları, siber komandoları olarak yetiştirilmesini sağlayacak bir proje geliştirilmesi,

- İsrail Ordusu'nun siber eğitim sistemi içerisinde yaptığı gibi seçilmiş öğrencilerin lise çağından itibaren eğitime alınmasının sağlanması,

- Ülkemizdeki yazılım ve bilgisayar bilimleri alanlında yetenekli çocuk ve gençlerin keşfedilmesi için programlar başlatılması,

- Bilgi güvenliği farkındalığı eğitimlerinin ilkokuldan itibaren, siber güvenlik ve algoritma geliştirme eğitimlerinin ise liseden itibaren verilmesi,

- Bilgisayar bilimleri alanında eğitim veren tüm lisans ve lisansüstü bölümlerde siber güvenlik eğitiminin verilmesi, böylelikle bilişim sistemi alanında çalışan herkesin siber güvenlik konusunda temelinin olmasının sağlanması,

- Özellikle üniversitelerde siber güvenlik eğitimlerinin en temel seviyede kalacak şekilde değil, ileri düzeyde ve teorik değil; pratiğe dayalı şekilde verilmesi hedeflenmelidir. Bu amaçla eğitim alan kişilerin, bir saldırı ile gerçek hayatta karşılaştıklarında alacakları aksiyonları kavraması sağlanması.

- Üniversitelerdeki eğitimin kalitesinin artırılması amacıyla akademi ve sektör işbirliğinin desteklenmesi,

- Siber güvenlik alanında çalışacak kişilerin, yabancı dil seviyelerinin de iyi olmasının amaçlanması,

- Siber güvenlik trendlerinin sürekli takip edilmesi, eğitimdeki yeni tekniklerin uygulanması,

- Ortak bir dil oluşturulması adına, TDK tarafından siber güvenlik sözlüğü oluşturulması,

- Siber güvenlik eğitimlerinin uygulamalı ve interaktif olacak şekilde yapılması. Yetiştirilen uzmanlara, gerçek hayatta karşılaşabilecekleri zorlukları çözebilme becerisinin pratik olarak verilmesi,

- Yüksek lisans ve doktora seviyesinde siber güvenlik bölümlerinin artırılmasının teşvik edilmesi,

- Siber güvenlik elemanı yetiştirecek ve sertifikalandıracak eğitim programları ve bağımsız kuruluşların desteklenmesi,

- Üniversitelerde siber güvenlik alanında akademik çalışmalar yapılmasının ve Türkçe kaynak eksikliğinin giderilmesinin teşvik edilmesi,

- Üniversitelerde siber güvenlik alanında projelerin geliştirilmesi ve yeni fikirler üretilmesinin teşvik edilmesi,

- Kamu kurumlarındaki siber güvenlik uzmanı eksiğinin giderilmesi için özel sektörden faydalanılması için özel sektör ile kamu kurumları arasında öğrenci değişimi gibi siber güvenlik uzmanı değişim programı uygulanması,

- Yine siber güvenlik alanındaki uzman eksiğini giderilmesi ve olası bir saldırı durumunda destek alınması amacıyla Hindistan'da uygulandığı gibi siber güvenlik uzmanı veritabanı oluşturulması ve uzmanlara ait iletişim bilgileri ile uzmanlık alanlarının tutulması,

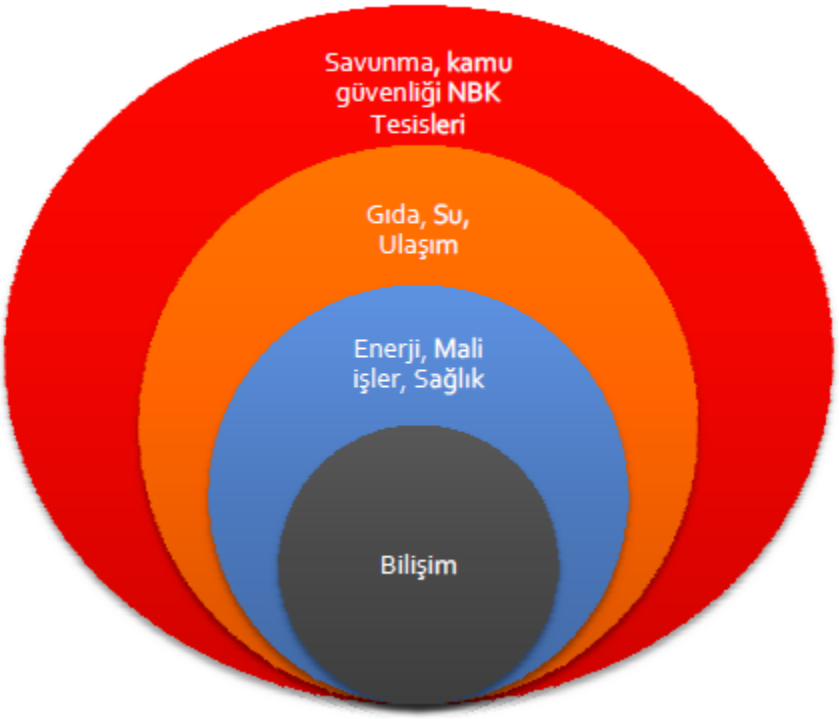
- Hackerların sahip oldukları yetenekleri lehe çevirmek ve sisteme bir hackerın gözünden bakabilmek adına, hackerların, devlet için çalışmasını teşvik edecek projelerin geliştirilmesi,

- Kamu kurumlarında çalışanların teknik bilgi eksiğini giderilmesi ve güncel bilgilerin takibinin sağlanması için, yurt dışında siber güvenlik eğitiminde iyi noktada olan kurumlara, belirlenen çalışanların gönderilmesi ve bu çalışanların döndüklerinde öğrendiklerini Türkiye'deki diğer çalışanlara aktarması şeklinde gerçekleşecek bir öğrenme ağı oluşturulması, önerilmektedir.

IX. Kritik Altyapıların Korunması

Kritik altyapılar, bir ülkenin ve ülkenin her bir şehrinin ama özellikle de gelişmiş şehirlerin can damarlarıdır ve şehirlerin sosyoekonomik yapısı ile yakından ilintilidir. Kritik sistemler denildiğinde, havalimanları, metrolar, gemiler, nükleer santraller, elektrik santralleri, telekomünikasyon sistemi, bankacılık sektörü, savunma birimleri, gaz ve su depolama ve dağıtım şebekeleri

gibi başlıklar akla gelmelidir.Gelişen teknoloji ile bu sayılan sistemlerin kontrolü, çalışması ve bakımı da gelişmiştir ve gelişmeye devam etmektedir. Söz konusu sistemler, bilgisayar sistemleri ile takip edilmektedir. Sistemlerin bilgisayarlar ile korunması ve yönetilmesi için projeler geliştirilirken, siber güvenlik tarafları ne yazık ki zayıf kalmış, üzerine düşünülmemiştir. Şekil 10'da anlatıldığı gibi, bilişim ve kritik alt yapılar birbiri ile iç içe geçmiş vaziyettedir.



Şekil 10: Kritik yapıların birbiri ile ilişkileri

Teknoloji, gelecek yıllarda karşılaşılması muhtemel savaş aracı haline gelmiştir. Karada, havada ve denizde kullanılan savaş silahlarının yanında dördüncü nesil savaş silahı olarak teknoloji gösterilmektedir. Teknolojiden kasıt, teknolojik aletlerin ve sistemlerin bertaraf edilmesi yoluyla saldırı düzenlenmesidir. Olası bir siber saldırı veya siber savaş durumunda sistemlerden birine veya birkaçına yapılacak bir saldırının bertaraf edilememesi çok büyük kargaşaya hatta felaketlere sebep olabilir. Bu nedenle siber güvenlik alanında çalışmalar yürütülürken en önem verilmesi gereken adım, kritik sistemlerin korunmasının ve savunmasının sağlanması olmalıdır.

Kritik sistemlerin yönetilmesini ve kontrolünü sağlayan sistemlere SCADA denilmektedir. Bu sistemlerin kullanımı, güvenliğinin sağlanması şartıyla, şebekelerin yönetilmesinin kolaylaşması, iş gücü ihtiyacının azalması bakımından gereklidir. SCADA sistemlerini, ilk yıllarında kullanılan protokollerin sisteme özel olması nedeniyle nispeten daha güvenlikli olmasına ve güvenliğinin sağlanması için ekstra çaba gerektirmemesine rağmen; gelişen teknoloji ile günümüzde ağ tabanlı olarak çalışan SCADA sistemlerine evrilmişlerdir. Bu da sistemin kendisine özel protokolkullanmayıp, genel protokoller kullanması anlamına gelmektedir. "SCADA sisteminde kullanılan iletişim hattına bağlı olarak kullanılan RTU[61]ve dağıtılmış saha ekipmanları arasında değişik haberleşme protokolleri kullanılabilmektedir."[62] Popüler protokollerin kullanımı da siber güvenlik zafiyeti yaratmaktadır. Diğer yandan, günümüzde internet kullanmayan sistemlerin dahil saldırıya uğramasının mümkün hale geldiği düşünülürse, her durumda kullanılan sistemin güvenliğinin sağlanmasının son derecede önemli olduğuna kanaat getirilecektir. SCADA sistemleri, kullanım amacına ve alanın büyüklüğüne göre kablolu veya kablosuz olarak kurulmaktadır. Çok büyük sistemlerin kablolu iletişim ile kullanılması efektif olamayacağından ya tamamen kablosuz ya da kablolu-kablosuz karma şekilde dizayn edilebilmektedir. Kablolu sistemlerde fiber optik kablo tercih edilirken, kablosuz sistemlerde ADSL, DSL, RF, uydu iletişim, GSM, GPRS, 3G hatları gibi teknolojiler tercih edilmektedir. SCADA sistemlerinde hangi teknolojinin kullanılacağına, gerek duyulan hız, maliyet ve güvenilirlik parametrelerine göre karar verilmelidir ve güvenliğin sağlanabilmesi için yedek bir hat ile kurulması sağlanmalıdır.

Bu çalışma kapsamında, SCADA sistemlerinin güvenliğinin sağlanabilmesi için kritik sistemlerin güvenliği alanında özellikli (spesifik) çalışmaların sektörel SOME'lerin çalışma alanına dahil edilmesi önerilmektedir. Bunun birinci amacı, yapılan çalışmaların tek elde toplanmasının sağlanmasıdır. İkinci ve en önemli amacı ise SCADA sistemlerinin güvenliğini sağlama işinin her sektör tarafından ayrıca yapılmasının gerekliliğidir. Kritik yapılar yukarı bahsedildiği gibi sektör bazında ayrıştırılmalı ve her sektörün sektörel SOME'si bu sektöre ait SCADA

[61]Remote Terminal Unit
[62]Kara, Mehmet, Çelikkol, Soner. "Ağ ve Bilgi Güvenliği Sempozyumu-Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği". (2011)

sistemlerinin korunması ve korunma yöntemlerinin geliştirilmesi ile görevlendirilmelidir. Hatta Sektörel SOME'ler de bu sistemler üzerindeki çalışmalarını kendi içlerinde kategorize ederek çalışmalıdır. Böylece her alanda güvenliği sağlamaya çalışan bir kurum/grup yerine, bir sektörün siber güvenliğinde uzmanlaşmış birçok kurum/grup oluşturulmalıdır. Siber güvenlik alanında çok iyi bir noktada bulunan ABD, kritik sistemlerinin güvenliğini bu şekilde sağlamaktadır.

Oluşturulması önerilen kritik sektör kırılımları şunlardır:

- kimya,
- ticari tesisler,
- iletişim,
- su/baraj sistemleri,
- savunma sistemleri,
- enerji,
- finans/bankacılık,
- gıda ve tarım,
- hükümet kurumları,
- sağlık,
- bilgi teknolojileri,
- nükleer,
- ulaşım,
- su ve atık su

Sektörel SOME'lerin çalıştıkları sektör için, o sektörün işletmecilerinin çalışmalarını düzenlemek, teftiş etmek, standartlar oluşturmak, kılavuz yayınlamak, kritik sistemlerin korunması için teknik destek vermek ve sürekli gelişimi sağlamak gibi çalışmalar yürütmesi gerekmektedir. Bu amaçla, daha önceki bölümlerde bahsedilen İngiltere'nin kritik altyapıları korumaktan sorumlu birimi CPNI'nın yapısı ve çalışmaları incelenebilir. Kritik altyapılara karşı gerçekleşebilecek saldırılar için olası senaryoların hazırlanması ve tehdit değerlendirmesi yapılması, daha önce bahsedilen erken uyarı sistemi ile kritik altyapıları işleten kurumların entegrasyonunun sağlanması, olası bir saldırıda savunma yapacak ve saldırıyı bertaraf edecekteknik yeteneklerin kurumlara kazandırılması, gerekli bilgilerin kategorize edilmesi ve her bir kurumun siber güvenlik standartlarına uygun hale gelmesi sağlanmalıdır. Kritik sistemleri işleten kurumlara, belirli aralıklarla teftişler yapılmalı ve tatbikatlar düzenlenmelidir. Bu kurumlarda sadece siber güvenlik alanında çalışan personelin değil, tüm personellerin bilgi güvenliği konusunda farkındalığı artırılmalıdır. Çünkü tehdide karşı 'antrenmanlı' olmayan kurumlar, savunma yapmada zayıf ve yetersiz kalacaktır.

İnternet aracılığı ile gelebilecek saldırılar, maddi amaçlı olabileceği gibi askeri amaçlı da olabilecektir. Siber güvenlik alanlında hala tartışılan noktalardan biri, siber saldırıların silahlı saldırı ile bir tutulup tutulamayacağıdır. Cenevre Sözleşmesi'nde alınan karara göre sivil hedeflerin bombalanmasının yasak olması gibi sivil kurumlara siber saldırının da yapılmaması üzerinde tartışmalar sürmektedir. Ayrıca, günümüzde birçok ülke siber güvenlik alanında yaptığı çalışmalara dair sınırlı bilgi paylaşmaktadır ve siber güvenlik konusunda şeffaflığın sağlaması da tartışma konularından biridir.[63] Gelecekte bu konularda ortak bir mutabakat çevresinde buluşulur mu bilinmez; ancak o zamana kadar özellikle saldırıya uğraması durumunda halkın hayatını sekteye uğratacak sistemlerin korunurluğunun garanti altına alınması gerekmektedir.

X. Kriz Yönetimi Planı Oluşturulması

Siber saldırılar ve siber terörizme karşı kriz yönetimi planı oluşturulmalıdır. Olası bir saldırı anında, gerekli müdahalenin yapılabilmesi için rollerin ve

[63]Karakuş, Cahit. "Kritik Alt Yapılara Siber Saldırı"

yetkilerin net olması, en önemlisi müdahalenin yapılması için kullanılacak standartların belirlenmesi gerekmektedir. Yaşanabilecek senaryoların belirlenmesi ve her bir senaryo için acil durum müdahale planlarının oluşturulması gerekmektedir. Hangi saldırı türünde hangi tepkilerin verileceği belirlenmelidir. Önemli ve sıklıkla kullanılan sistemlerin, kesintisiz çalışabilmesi için önemler alınmalı, veritabanı gibi sistemlerin, uygun lokasyonlarda yedekleri bulundurulmalıdır. Erken uyarı sistemleri kullanılmalıdır. Saldırı durumunda kullanılması veya saldırı sonrasında saldırganın tespiti, hasarın tespiti veya saldırıya sebep olacak açığın tespiti için kullanılmak üzere kesinlikle log tutulması sağlanmalıdır. Saldırı sonrasında ders çıkalrılması amacıyla raporlama sistemi, standardize edilmelidir.

XI. Diğer Öneriler

- Türkiye'nin siber güvenlik alanında yapması gerekenler listesinin en başında, siber güvenlik alanında yapılan çalışmaların devamlılığını sağlamak ve oluşturulan Siber Güvenlik Strateji Belgeleri'nde alınan kararların uygulanması konusunda kararlı olmak gelmektedir.

- Siber güvenlik alanında çalışacak tüm kurumların yetki ve sorumluluklarının kesin olarak belirlenmesi gerekmektedir.Sistemdeki kurumların yetkilerinin belirsiz olması veya bir ekibin birden çok sorumluluğunun olması yeterli etkinin sağlanmasını engellemektedir.

- Siber güvenlikle ilgili projelerin desteklenmesi ve özellikle yerli yazılım üretilmesinin desteklenmesi gerekmektedir. Zira dışarıdan alınan yazılımlar ile güvenliğin tam olarak sağlanması mümkün değildir. Bu amaçla İsrail'in yaptığı gibi siber güvenlikle ilgili şirketlerin ve akademik kadronun bir araya getirilmesi sağlanabilir. Bu amaçla hali hazırda bulunan Teknoparklar kullanılabilir.

- Teknolojinin ilerlemesi ile gelinen noktada, cep telefonlarından, televizyonlara; elektronik medikal cihazlardan, giyilebilir teknolojilere birçok elekkronik aygıt veri depolamaktadır. Bahsedilen veri ise gün geçtikçe kıymetlenmekte ve sanal hırsızlıklara kapı aralamaktadır. IDC'ye göre 2016 yılı sonuna kadar, Dünya üzerindeki bilişim ağlarının %90'ının güvenliği aşılmış

olacaktır.[64] Dolayısıyla Türkiye'de de verinin korunması, ayrı bir çalışma alanı olarak belirlenmeli ve projelendirilmelidir.

- E-Ticaret sitelerinin ülkemizde de son zamanlarda artış gösterdiği düşünülürse, bu sektörün güvenliğinin sağlanmasının da çok önemli olduğu görülebilir. Özellikle küçük çaplı e-ticaret sitelerine siber güvenlik desteği verilmeli ve sistemlerinin kontrolü sağlanmalıdır. Daha önce bahsedilen Siber Güvenlik İnsiyatifi'nin kobiler ile ilgili projesine e-ticaret siteleri de dâhil edilmelidir.

- Hükümet sistemlerinin büyük kısmının sayısal ortama taşındığı günümüzde vatandaşların bilgilerinin güvenliği de kritik öneme sahiptir. E-devlet sistemlerinde yaşanacak bir veri hırsızlığını engellemek için e-devlet sitelerinin güvenliğine azami önem gösterilmelidir.

- Siber güvenlikle ilgili proje yarışmaları düzenlenmelidir.

- Ülkenin beyaz şapkalı hacker'ları tespit edilip, bilgilerini ülke yararına kullanmaları sağlanmalıdır. Unutulmamalıdır ki; hacker'lar, internetin bağışıklık sistemidir.

- Siber güvenlik alanında savunma ve saldırı tekniklerini geliştirmek amaçlı bu alanlarda yarışmalar düzenlenmelidir.

- Özellikle siber güvenlik alanında gelişmiş olan diğer ülkelerle, bilgi paylaşımı ve teknik destek almak veya vermek amaçlı siber güvenlik anlaşmaları yapılmalıdır.

- Türkiye'nin NATO'nun Mükemmeliyet Merkezi üyesi olması çalışmaları kısa süre içerisinde tamamlanmalıdır.

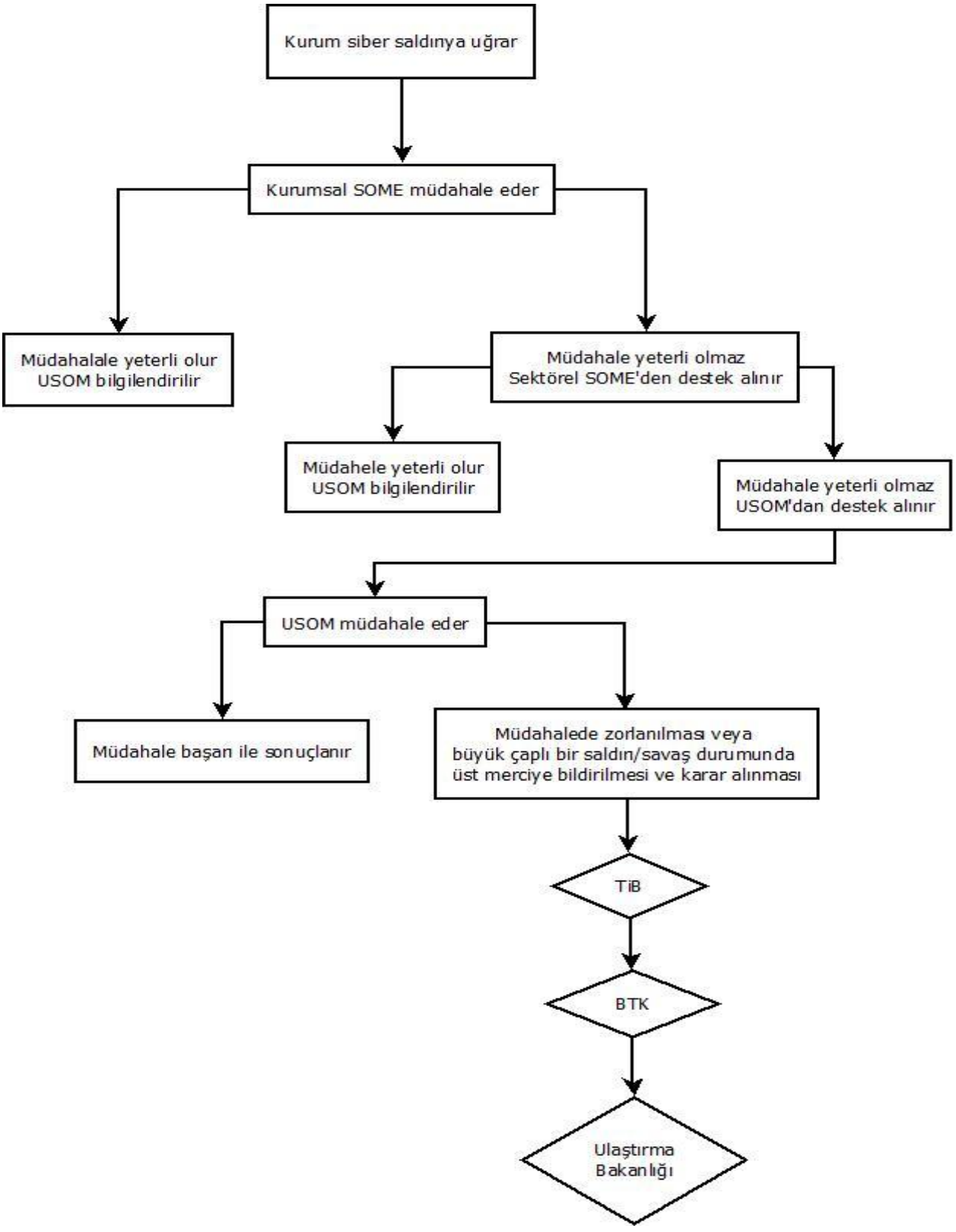
- NATO'nun siber güvenlikle ilgili stratejik plan oluşturma toplantılarına en azından gözlemci olarak katılım sağlanmalıdır.

- Hem özel sektörde hem de devlet kurumlarında, sadece güvenlikle ilgili birimlerin çalışanlarının değil, tüm çalışanların siber güvenlik farkındalığı

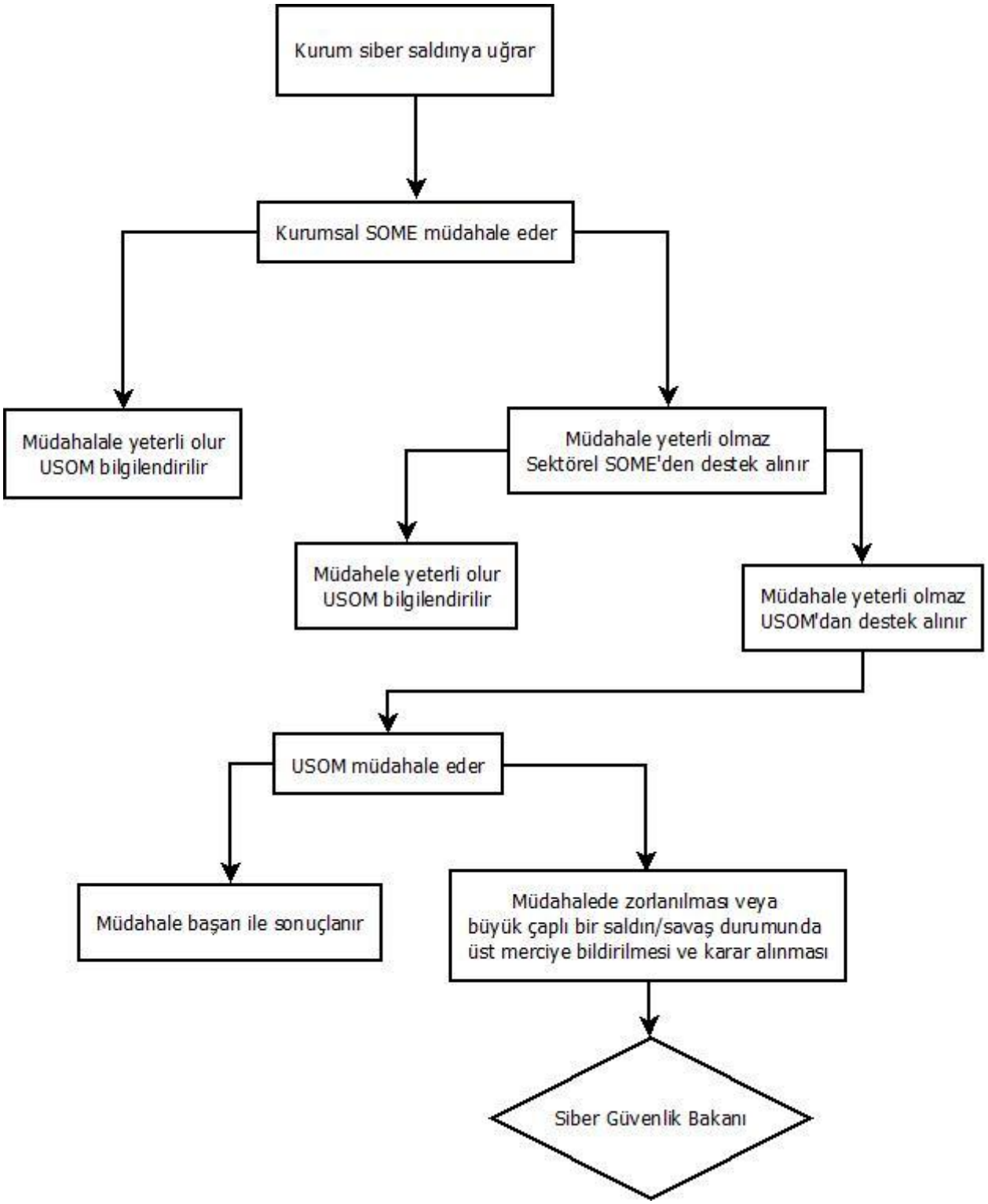
[64] Anonim. "Zetta-Byte'ın Yılı" (2016 Ocak). Popular Science

kazanması için farkındalık eğitimleri verilmelidir. Hatta sadece beyaz yakalı değil, mavi yakalı çalışanların da bu eğitimleri alması sağlanmalıdır.

XII. Örnek Olay Üzerinden Türkiye'nin Mevcut Siber Savunma Sistemi ve Önerilen Siber Savunma Sistemi



Şekil 11: Türkiye'nin Mevcut Siber Savunma Olay Akışı



Şekil 12: Türkiye için Önerilen Siber Savunma Olay Akışı

5. Sonuç

Teknoloji büyük bir hızla gelişmekte ve evrilmektedir. Nasıl ki 15 yıl içerisinde bilgisayarla olan ilişkimiz her mahallede bir bilgisayarın olması durumundan her evde iki-üç tane dizüstü bilgisayar, birden fazla akıllı telefon olma durumuna geldiyse, ilerleyen yıllarda da bu yönde bir gelişim olacaktır. Günümüzde kullanılmaya başlanan bulut bilişim ve mobil cihazların güvenliği bile henüz tam olarak sağlanamamışken, ilerleyen yıllarda nesnelerin interneti (IOT)[65] kavramının gelişmesi ve makine-makine (M2M)[66] etkileşimi ile çalışan sistemlerin gündelik hayatımıza girmesiyle hem bu sistemlerin güvenliğini sağlamak daha zor olacağı için siber güvenlikteki yük artacak; hem de sistemlerin saldırıya uğraması durumunda yaşanacaklar ve alınacak aksiyonlar karmaşıklaşacaktır. Bu konuda önemli bir nokta da mevcut durumda teknoloji şirketlerinin güvenli yazılımlar üretmeye çalışması ve devletlerin de siber güvenlikle ilgili alınan kararlar doğrultusunda uyguladıkları yaptırımlar nedeniyle yenilenme hızının yavaşlamasıdır. Dolayısıyla hem güvenli bir sistem kurmak hem de teknolojinin hızına yetişmek ciddi bir çaba gerektirmektedir. Bilgiye erişmek her geçen gün daha kolaylaştığı için sistemlere saldırı düzenlemek de daha maliyetsiz hale gelmektedir. İngiltere Ulusal Suç Dairesi (NCA)'nin açıklamasına göre, siber sanıkların yaşı 17'ye kadar düşmştür.[67] Devletlerin saldırma potansiyelleri görmezden gelinerek; sadece bireysel saldırılar baz alındığında bile, gelecekte düşük maliyetli; ancak karşıdaki kişiye/kuruma çok ciddi zararlar veren saldırıların sayısının aratacağı çok net görülmektedir. Bu nedenle, şimdiden gelecek için hazırlıklı olunmalı ve öngörülü bir siber güvenlik eylem planı ve stratejisi oluşturulmalıdır. Teknoloji büyük bir hızla ilerlemekte ve yenilenmekte; bu ilerleme ve yenilenme ise riskleri beraberinde getirmektedir. Gelişmiş bir ülkenin yeniliklerden faydalanmaması ve kendisini geliştirmemesi de bu yeniliklerin getirdiği riskler nedeniyle ciddi zararlara uğraması da kabul edilebilir bir durum değildir. Özellikle günümüzde yeni kullanılmaya başlanan ve gelecekte hayatımızın merkezinde yer alacağı düşünülen teknolojiler olan, M2M, IOT, giyilebilir kıyafetler, teknolojik arabalar vb. teknolojiler için veSCADA

[65]Ayrıntılı bilgi için bknz. Greengard, Samuel. "The Internet of Things" (2015).
[66]Ayrıntılı bilgi için bknz. http://www.m2mturkiye.com/m2m-nedir-machine-machine/ Erişim tarihi: 04.01.2016
[67] Anonim. "Siber Suçlar Çocuk Oyuncağı Oldu" (2016, 3 Ocak). Erişim tarihi: 04.01.2016. http://siberbulten.com/strateji-guvenlik/siber-suclar-cocuk-oyuncagi-oldu/

sistemlerinin korunması gibi çok önemli konular için ayrı çalışma grupları oluşturularak, alınacak aksiyonlar belirlenmelidir. Siber güvenlik konusunda ciddi yol almış ülkelerin yaptıkları örnek alınarak, başarılı olan uygulamaların Türkiye'de de gerçekleştirilmesi ve daha ileriye götürülmesi hedeflenmelidir. Siber güvenlik alanında hem hukuksal hem teknik bir süreç başlatılmalı ve Türkiye'nin sahip olduğu potansiyelin değerlendirilmesi amaçlanmalıdır. Bu amaçla, var olan siber savunma süreçlerinin geliştirilmesi ve yeni süreçlerin tasarlanması; risk yönetiminin mutlaka hayata geçirilmesi önerilmektedir. Ayrıca siber güvenlikte iyi bir noktaya gelmenin en önemli koşulunun eğitimli personellerin varlığı olduğundan hareketle, siber güvenlik alanında yapılan çalışmaların temel çalışmalarından biri, personellerin siber güvenlik eğitimi alması ve sertifikalandırılma süreçleri ve yeni nesil siber güvenlik uzmanlarının yetiştirilmesi konularına yoğunlaşan eğitim çalışması olmalıdır. Siber güvenlikte, siber güvenlik uzmanı ve kullanılan yazılımlar açısından dışa bağımlı olmanın, daima siber tehditlere karşı zayıf olmak anlamına geldiği unutulmamalıdır. Son yıllarda ülkemizin siber güvenlikten sorumlu kurumları, siber güvenlik alanındaki gelişmelerini yavaşlatmışlardır. Siber güvenlik çalışmalarında danışmanlık rolünü üstlenmesi için kurulan Siber Güvenlik Kurulu, 2013 yılında 2 kere toplamış; 2014 ve 2015 yıllarında ise hiç çalışma yapmamıştır.[68] Ayrıca teoride siber saldırılara müdahale etmesi bekelenen USOM ve SOME'ler, son yıllarda sadece bilgilendirme yapmaktadır. Teknolojinin hayatın ayrılmaz bir parçası olduğu günümüzde, devlet kurumlarına olan bakış açısının güncellenmesi ve siber güvenlik alanının, bugün ve gelecekte devletin en önemli kurumlarından biri olması gerektiği gerçeği göz ardı edilmemelidir.

Siber güvenlik alanında yaptırımlara devam edilirken, diğer yandan siber güvenliği sağlamak amacıyla atılan adımların toplumun teknoloji kullanımının engellenmesine sebep olmamasına dikkat edilmelidir. Siber uzayda güvenliğini sağlayabilen, gerekli savunmayı yapabilecek yetkinliğe sahip bir ülkenin aynı zamanda temel hak ve özgürlüklerin korunması, ifade özgürlüğünün engellenmemesi, kişisel verilerin korunmasının sağlanması gibi temel konularda da net olması gerekmektedir. Veri korumasının sağlıklı bir şekilde sağlanamadığı

[68]http://www.turk-internet.com/portal/yazigoster.php?yaziid=42765

bir ülkenin, siber güvenlik konusunda ne kadar iyidurumda olursa olsun, uluslar arası arenada diğer ülkelerin paydaşı olması mümkün değildir.