SİBER GÜVENLİK RAPORU

Mayıs 2012, İstanbul

İÇİNDEKİLER

SİBER GÜVENLİK RAPORU VE SİBER GÜVENLİK ÇALIŞMA GRUBU HAKKINDA 3
Siber Güvenlik Çalışma Grubu Kadrosu: 3
SİBER GÜVENLİK RAPORU – YÖNETİCİ ÖZETİ 4
SİBER GÜVENLİK POLİTİKALARINA VE UYGULAYICI KURUMLARA DÜNYADAN ÖRNEKLER 5
HİNDİSTAN 5
AMERİKA BİRLEŞİK DEVLETLERİ 12
ÇİN 18
ESTONYA 22
BİRLEŞİK KRALLIK 30
ALMANYA 33
İSRAİL 39
SİNGAPUR 41
NATO – Kuzey Atlantik Antlaşması Örgütü 43
ITU (Uluslar arası Telekomünikasyon Birliği) 48
AVRUPA BİRLİĞİ (AB) 55
DÜNYADAKİ BAŞARILI ÖRNEKLER ÇERÇEVESİNDE TÜRKİYE CUMHURİYETİ İÇİN ÖNERİLER 60
HİNDİSTAN 60
AMERİKA BİRLEŞİK DEVLETLERİ 60
ÇİN 65
ALMANYA 65
ITU 66
BİRLEŞİK KRALLIK 68
AVRUPA BİRLİĞİ 68
SİNGAPUR 69

SİBER GÜVENLİK RAPORU VE SİBER GÜVENLİK ÇALIŞMA GRUBU HAKKINDA

Bu çalışma Yrd. Doç. Dr. Leyla Keser Berber tarafından verilen görev çerçevesinde Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü bünyesinde siber güvenlik alanında araştırmalar yapan veya fiilen çalışan uzmanların oluşturduğu 'Siber Güvenlik Çalışma Grubu' tarafından hazırlanmıştır. Siber Güvenlik Çalışma Grubu bünyesinde, çoğunluğu Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı öğrencileri olmak üzere, devlet sektörünün çeşitli birimlerinde ve özel sektörde çalışan 11 uzman bulunmaktadır. Yaklaşık 8 haftalık yoğun bir çalışma süreci içerisinde taslak olarak hazırlanan bu çalışmada, özenle seçilmiş olan çeşitli ülkelerin siber güvenlik politikaları incelenmiş, bu politikaları hangi kurumlar ile uyguladıkları saptanmıştır. Ayrıca bu uygulamaların hukuki altyapılarına da değinilerek, başarılı örnek modeller çerçevesinde Türkiye Cumhuriyeti'nin siber güvenliğinin geliştirilmesine katkı sağlayabilecek öneriler sunulmuştur.

Siber Güvenlik Çalışma Grubu Kadrosu:

İlke Deniz DURNA: Çalışma Grubu Genel Koordinasyonu + Çin ve Hindistan İncelemesi

Emin ÇALIŞKAN: NATO ve Estonya İncelemesi + Genel Analiz

Ahmed Furkan GÜL: Çin ve ABD İncelemesi

Oktay ONAY: İsrail İncelemesi

Merve GÖZÜKÜÇÜK: ITU ve AB İncelemeleri

Burak TAŞÇI: Fransa ve AB İncelemeleri

Zeynep Sena DÖVER: ITU İncelemesi

Burak ÇELİK: Almanya İncelemesi

Batu Yakup KINIKOĞLU: Birleşik Krallık İncelemesi

Ahmet ÜNAL: ABD İncelemesi

Mehmet Bedii KAYA: Singapur İncelemesi

SİBER GÜVENLİK RAPORU – YÖNETİCİ ÖZETİ

Günümüzde hızla artan siber tehditler nedeniyle, birçok ülke güvenlik politikalarının içerisinde önemli bir başlık olarak siber güvenliğe yer vermeye başlamıştır. Bu ülkelerden bazıları ekonominin, sosyal yaşamın ve milli güvenliğin sanal dünya ile giderek iç içe girmesi sebebiyle, siber güvenlik alanına büyük yatırımlar yaparak bu alanda çalışacak kadroları yetiştirmek için çeşitli stratejiler geliştirmektedirler. Bunların dışındaki ülkeler ise daha geriden gelişmeleri takip ederek, başarılı örnekleri saptadıktan sonra onları kendilerine uyarlayarak kamu ve özel sektördeki ağların güvenliğini sağlamaya çalışmaktadır.

Hazırlanan bu *Siber Güvenlik Raporu*'nda yeni siber savunma güvenlik politikaları oluşturup bu konuda detaylı stratejiler geliştiren, bu stratejileri uygulayacak kurumları oluşturan ve kurumların çalışmalarıyla ilgili hukuki altyapıları düzenleyen ülkelerin önde gelenleri tek tek incelenmiş ve Türkiye Cumhuriyeti açısından örnek olabilecek uygulamalar öneri olarak sunulmuştur.

İncelenen ülkeler arasında **Amerika Birleşik Devletleri, Almanya, Fransa, Birleşik Krallık ve Estonya** gibi NATO üyesi ülkelerin yanısıra, ortaya özgün ve gelişmiş bir siber güvenlik modeli koyan **Hindistan, Çin, Singapur ve İsrail** gibi ülkeler de mevcuttur.

Ülke bazlı incelemenin yanısıra, **NATO, AB ve ITU** gibi uluslararası örgütler de detaylı olarak incelenmiş ve siber güvenlik alanında hangi noktada oldukları saptanarak, Türkiye Cumhuriyeti açısından model oluşturabilecek öneriler sıralanmıştır.

Siber güvenliğin en üst düzeyde sağlanabilmesi için;

- Siber güvenlik politikasının oluşturulması,
- Devletin çatısı altında uygulayıcı kurumların oluşturulması,
- Daha sonrasında uyum içerisinde çalışabileceği bir mekanizmanın kurulması,
- Bu yapıların esnek ve hızlı bir biçimde çalışmalarını sağlayabilecek hukuki altyapının oluşturulması gerekliliği,
- Ülkemizde bu alanda hem kamu hem de özel sektörde çalışacak nitelikli personel ihtiyacının karşılanabilmesi için üniversitelere düşen roller,
- En son gelişmeleri takip edip siber güvenlik alanında en ileri düzeyde savunma yapabilmek için AR-GE merkezlerinin kurulması gerekliliği,

bu raporda ön plana çıkan önemli noktalardır.

SİBER GÜVENLİK POLİTİKALARINA VE UYGULAYICI KURUMLARA DÜNYADAN ÖRNEKLER

HİNDİSTAN

Hindistan yaklaşık 1.173.000.000 kişilik nüfusu ile Çin'den sonra dünyanın en kalabalık 2. ülkesi olmasının yanı sıra, Çin ile birlikte yakın gelecekte güç dengelerini önemli oranda değiştireceği tahmin edilen, dünyada politik ve stratejik anlamda en önemli ülkelerden birisidir.[1] Yoğun nüfusunun yanında, bilişim sektöründeki gelişmeler ve yatırımlar sebebiyle Hindistan, siber güvenlik alanına birçok ülkeden daha fazla önem vermeye başlamış ve bununla ilgili olarak çeşitli düzenlemelere gitmiştir.

Bilişim sistemlerine ve bilgi güvenliğine karşı giderek büyüyen tehditleri karşılayabilmek için, Hindistan Devleti Inter Departmental Information Security Task Force (ISTF) isimli kuruluşu oluşturmuş ve Ulusal Güvenlik Konseyi (National Security Council) ile birlikte en üst düzeyde yetkilendirmiştir. Böylece kapsamlı bir Ulusal Siber Güvenlik Politikasının inşasına başlanmıştır. Bu çerçevede ISTF'nin yaptığı öneriler doğrultusunda aşağıdaki konu başlıklarıyla ilgili devlet düzeyinde çalışmalar yapılmaya başlanmıştır[2]:

- Ulusal bilgi güvenliği tehdit algılamalarının saptanması
- Kritik altyapıların korunması
- Bilgi güvenliğinin sağlanması için gerekli yasal düzenlemelerin hazırlanması
- Siber güvenlik konusunda farkındalık yaratılması ve ilgili personelin eğitimi
- Siber güvenlik konusunda araştırma ve geliştirmelerin desteklenmesi ve bu çalışmalara özel sektörün ve üniversitelerin de dahil edilmesi

[1] Country Reports – India, http://www.countryreports.org/country/India.htm.
[2] Cyber Security Strategy, Department of Information Technology (India), http://mit.gov.in/content/cyber-security-strategy.

Bu çalışmaların yanında, Hindistan Devletine ait ağların ve kritik altyapıların korunması için Bilgi Güvenliği Çerçeve Politikası hazırlanmıştır. Ulusal çapta yürütülen bir Bilgi Güvenliği Farkındalığı ve Eğitimi Kampanyası düzenlenmiştir ve bu kampanya devam etmektedir.

Ülkenin siber uzayını güvenli hale getirebilmek için, Hindistan ana hedef olarak şunları koymuştur:

- Ülkenin kritik bilişim sistemleri ve altyapılarına yönelik saldırıların önlenmesi,

- Siber saldırılar karşısındaki zafiyetin azaltılması,

- Siber saldırılardan doğan zararların en aza indirilmesi ve müdahale/düzeltmelerin en hızlı şekilde yapılabilmesi.

Siber uzayın güvenli tutulabilmesi için uygulanacak eylem planı da aşağıdaki gibi belirlenmiştir:

- Adli bilişim sistemlerinin geliştirilmesi ve saldırı analizlerinin 7/24 esasına göre yapılması
- Ulusal açıdan kritik önemde olan altyapıların, ağların ve bilişim sistemlerinin korunması
- Erken saptama ve uyarı sistemlerinin geliştirilmesi
- Ekonomiye zarar verebilecek düzeydeki organize siber saldırılara karşı koruma sağlanması
- Kritik sektörlerdeki firmaların bilişim sistemlerinin güvenliklerini en üst düzeyde sağlayabilmeleri için onlara AR-GE desteğinin verilmesi.[3]

Siber güvenliğin sağlanmasına yönelik oluşturulan bu stratejinin yanı sıra, Hindistan Ulusal Güvenlik Konseyi Danışma Kurulu (National Security Council Advisory Board) sunduğu bir raporda, Amerika Birleşik Devletleri'nin oluşturduğu gibi merkezi bir siber komutanlığın kurulmasını önermiştir.[4]

[3] Cyber Security Strategy , Department of Information Technology - Government Of India http://mit.gov.in/content/cyber-security-strategy.
[4] James A. Lewis – Katrina Timlin, "Cybersecurity and Cyberwarfare", Center For Strategic and International Studies, 2011,p. 14.

1990'lı yılların sonuna doğru Hindistan ordusu, savaş doktrinine elektronik muharebe ve bilgi teknolojileri operasyonlarını da dâhil etmiştir. Bununla birlikte, bilgi teknolojileri, elektronik muharebe, kritik altyapıların korunması gibi konularda modernizasyona gidilmeye başlanmıştır.[5] Hindistan Savunma Bakanlığı bünyesinde, siber güvenlikten sorumlu olarak tayin edilmiş çeşitli birimler bulunmaktadır.[6] Ayrıca, Hindistan Savunma İstihbarat Teşkilatı (Defence Intelligence Agency – DIA) ve Ulusal Teknik İstihbarat İletişim Merkezi (National Technical Intelligence Communication Center) birlikte özel bir siber birlik oluşturmuş ve bu birliğe, devleti siber güvenlik ihlalleriyle ilgili olarak anında uyarma ve tedbir alma gibi bir görev vermişlerdir. Ayrıca, yurtdışından gelen siber saldırılara karşı cevap verme yetkisi de bu birliğe verilmiştir.[7] Bunların yanı sıra, Hindistan Savunma Araştırma ve Geliştirme Organizasyonu (Defence Research and Development Organization) elektronik muharebe sistemlerinin test edilmesi için iki tane tesis oluşturmuştur.[8]

2005 yılında Hindistan Ordusu tarafından ordunun bilgisayar ağlarının güvenliğinin sağlanması ve düzenli olarak denetlenmesi amacıyla Siber Güvenlik Kuruluşu (Cyber Security Establishment) oluşturulmuştur.[9] Ayrıca, Hindistan Ordusu 2010 Nisan ayında Askeri Telekomünikasyon Mühendisliği Üniversitesi bünyesinde, bir siber güvenlik laboratuvarı kurmuştur.

Hindistan ordusunun yanında, Hindistan Devleti'ne bağlı sivil birimler de siber güvenlik konusunda yoğun çalışmalar yapmaktadırlar. ISTF'nin önerileri doğrultusunda, 2004 yılının Ocak ayında Hindistan Acil Bilgisayar Müdahale Ekibi (Indian Computer Emergency Response Team – CERT-In) Hindistan Devleti'ne bağlı olan Bilgi Teknolojileri Departmanı (Department

[5] Charles Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Certain Nation States", Institute for Security Technology Studies, Dartmouth University, 2004, p. 41–45.
[6] Vinod Anand, "Integrating the Indian Military: Retrospect and Prospect", *Journal of Defence Studies*, vol. 2, no. 2, 2008, p. 37.
[7] Harsimran Singh and Joji Thomas Philip, "Spy game: India readies cyber army to hack into hostile nations' computer systems", *The Economic Times*, 6 Ağustos2010.
[8] "India to built two test ranges of electronic warfare systems", *Business Standard*, 24 Kasım 2010.
[9] Rajat Pandit, "Army gearing up for cyber warfare", *The Times of India.*

of Information Technology) tarafından bilgisayar güvenliğine ilişkin olaylara zamanında ve kapsamlı bir biçimde müdahale edilebilmesi amacıyla kurulmuştur.[10]

27 Ekim 2009 tarihinde yürürlüğe giren Hindistan Bilgi Teknolojileri Kanunu'nda yapılan değişiklikle birlikte (Kanunun 70. Maddesinin B Bölümü) CERT-In oluşumu, ülke çapındaki siber güvenlik ve acil müdahale durumlarıyla ilgili olan tüm konularda koordinasyonu sağlayan bir kilit kurum olarak yetkilendirilmiştir.[11] Hindistan Bilgi Teknolojileri Kanunu ayrıca genel olarak hacker saldırıları, bilişim sistemi altyapılarındaki güvenlik ihlalleri gibi durumlarla mücadelenin yasal altyapısını oluşturmaktadır. Kanunun 70. maddesindeki tanıma göre, kritik bilgi altyapısını doğrudan ya da dolaylı olarak etkileyen bütün bilgisayar ekipman veya kaynakları korunması gereken sistem şeklinde nitelendirilmiş ve CERT-In siber savunmayla ilgili gerekli müdahaleleri yapmak ile görevlendirilmiştir.[12]

Bugün CERT-In Hindistan Siber Uzayının gözetim altında tutulması çerçevesinde siber korunmanın sağlanması, Devlet düzeyinde ve kritik sektörlerde güvenlik standartlarının yükseltilerek buna uyum sağlanması ve güvence altına alınması, erken uyarı ve müdahale sistemlerinin faaliyete geçirilmesi, bu alanlarda bilgi paylaşımı ve işbirliğinin koordine edilmesi gibi önemli görevleri üstlenmiş durumdadır. CERT-In tarafından siber güvenliğe ilişkin çeşitli kılavuzlar ve eylem planları hazırlanmış ve tüm devlet kademelerinde yaygın bir biçimde dağıtılmıştır.

Kuruluşundan itibaren CERT-In Hindistan devletinin güvenlik bürokrasisindeki tüm kurumlarla işbirliği halinde siber güvenlik olaylarına müdahale etmekte, ayrıca dünya çapında ileri düzeyde uzmanlığa sahip siber güvenlik alanında çalışan birçok bilişim firmasıyla çeşitli işbirliği mekanizmaları oluşturmaktadır. Bunun yanı sıra, kurum bünyesinde adli bilişim

---

[10] Indian Cyber Security and Emergency Response, Northern Voices Online, http://nvonews.com/2010/01/15/indian-cyber-security-and-emergency-response/

[11] Information Technology (Amendment) Act 2008, of Communications and Information Technology – Government of India, http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

[12] Information Technology Act, Department of Information Technology – Government of India, http://www.mit.gov.in/content/information-technology-act

laboratuvarları oluşturulmuştur ve bu laboratuvarlarda en yeni zararlı kodların analizleri düzenli olarak yapılmaktadır.[13]

CERT-In 2010 yılında "Siber Saldırılar ve Siber Terörizme Karşı Kriz Yönetimi Planı" oluşturmuş ve bu planın tüm devlet bazında ve kritik sektörlerde uygulamaya geçirilmesi için çalışmalarına devam etmektedir. Bunun dışında kritik sektörlerde ve devlet kurumlarında siber saldırılara karşı direncin daha sağlam olması ve güvenlik omurgasının güçlendirilmesi için, kritik sektörlerde iş yapan firmalara, Hindistan Devleti tarafından, ISO 27001 Bilgi Güvenliği Yönetimi Standardı çerçevesinde iş organizasyonlarını yeniden oluşturmaları konularında bilgilendirmelerde bulunulmakta ve bu dönüşüm teşvik edilmektedir. Hindistan'da yaklaşık 246 firma ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardına uygunluk sertifikasına sahiptir ve bu firmalar genellikle bilgi teknolojileri, telekomünikasyon ve bankacılık gibi sektörlerde yer alan firmalardır[14]. CERT-In kanalıyla, devlet kurumlarına ve özel sektördeki firmalara düzenli aralıklarla penetrasyon testleri uygulanmakta ve böylece bilişim sistemlerinin hangi noktalarında açıkları olduğu saptanarak bunlara yönelik önlemler alınmaktadır.

CERT-In Hindistan Bilgi Teknolojileri Departmanına ulusal siber güvenlik stratejisi ve ulusal bilgi güvenliği yönetimi politikası oluşturulması konularında danışmanlık yapmaktadır. CERT-In gelecek için yol haritasını çizerken, sadece olaylara karşı müdahale mekanizmasının siber güvenliği sağlamada tam olarak yeterli olmayacağını, aynı zamanda proaktif bir siber güvenlik politikası oluşturularak gerçek zamanlı bilgi paylaşımına dayalı bir sistemin oluşturulması gerekliliğini saptamıştır. Böylece siber güvenlikle ilgili olay gerçekleşmeden belirli risk parametrelerine ulaşılacak ve gerçek zamanlı bilgi paylaşımına dayalı olarak olay engellenebilecektir.

Hindistan Hükümeti Basın Bilgi Bürosu, yaptığı yazılı bir açıklamada, Hindistan Siber Güvenlik Politikası kapsamında, hassas düzeyde ve devletin güvenliğini ilgilendiren gizli bilgilerin,

[13] About Indian Computer Emergency Response Team (CERT-In), Ministry of Communications and Information Technology – Government of India, http://www.cert-in.org.in/
14 Cyber Security Strategy , Department of Information Technology - Government Of India, http://mit.gov.in/content/cyber-security-strategy

internete bağlı olan bilgisayarlarda kesinlikle tutulmadığını açıklamıştır.[15] Özellikle Hindistan Dışişleri Bakanlığı'nın, yurtdışındaki misyonlarıyla yaptığı iletişim ve yazışmalar için özel güvenlik standartları geliştirilmiş, bu çerçevede görev yapan bütün personel özel bilgi güvenliği eğitimlerinden geçirilmiş ve bu eğitimler düzenli olarak belirli zaman aralıklarıyla devam ettirilmektedir.

National Informatics Center (NIC) isimli Hindistan Devletine bağlı kuruluş, Hindistan çapında ağ omurgasını sunmakta ve denetlemekte, ayrıca Hindistan Federal Devleti ve bünyesindeki federe devletlere, daha küçük idari birimlere ve belediyelere e-devlet hizmetleri sunulması konusunda destek vermektedir. Bu yüzden NIC altyapısının güvenliği Hindistan Devleti için kritik önemdedir.[16]

Bütün bu sayılanların dışında, Ulusal Güvenlik Veri Tabanı (National Security Database-NSD) isimli bir oluşum kurulmuş ve bünyesinde siber güvenlik ile ilgili ve ulusal kritik altyapıların ve bilişim sistemlerinin korunmasıyla ilgili çalışan güvenilir ve donanımlı uzmanların listesi oluşturulmuştur. Bu veri tabanı sayesinde ülkedeki kritik sektörlerde görev yapmak isteyen kişilerin de belli testlerden ve güvenlik soruşturmalarından geçmeleri sağlanmakta ve böylece özel sektörde de bilgi güvenliği açısından insan kaynaklı hataların en aza indirilmesi hedeflenmektedir. Daha yüksek pozisyonlarda ve önemli noktalarda çalışmak isteyen uzmanların, Ulusal Güvenlik Veri tabanı bünyesindeki konumu ve eylemlerine bakılmakta ve ona göre karar verilmektedir.

NSD, Hindistan tarafından da desteklenen kar amacı gütmeyen Information Sharing and Analysis Center (ISAC) isimli bir sivil toplum kuruluşunun projesi olarak geliştirilmiştir. ISAC siber güvenlik alanında kamu-özel sektör işbirliğinin Hindistan'daki başarılı bir örneğidir. NSD'nin amacı, ülkenin neresinde olursa olsun, devletin çok hızlı bir biçimde müdahale etme olanağı olmayan siber güvenlik olaylarında, sivil uzmanların da olaylara müdahale etme kapasitesinin kullanılmasıdır. Bir diğer amaç ise, bilgi güvenliği ve siber güvenlik alanında

[15] Crisis Management Plan for Cyber Attacks, Press Information Bureau – Government Of India, http://pib.nic.in/newsite/erelease.aspx?relid=61597

[16] Col SS Raghav, Cybersecurity in India's Counter Terrorism Strategy, p.3

çalışan nitelikli kişilerin envanterinin çıkarılması ve kritik alanlarda NSD'deki güvenilirlik seviyelerine göre işlerde çalışmalarının sağlanmasıdır.[17]

[17] National Security Database, An ISAC Project supported by the Government of India, http://nsd.org.in/web/about/

AMERİKA BİRLEŞİK DEVLETLERİ

Amerika siber uzayın oluşturduğu yeni gerçeklere kurumsal tepki veren önder ülkelerden biri olarak görülmektedir. Devlet olarak siber uzayın kurulmasına destek çıkarak ve kullanımını teşvik ederek diğer ülkelere örnek olmuştur. Özellikle Avrupa ve Asya'daki ülkelere siber sorunlar ile başa çıkılması konusunda örnek teşkil ederek bir rol model haline gelmiştir. Her ne kadar Amerika siber tehlike ve tehditlere karşı muhafaza sistem ve altyapısına sahip en güçlü ülkelerden biri olarak görülse de şu anda uygulanmakta olan programlar, sistem ve altyapıların günümüzdeki tehlikelere karşı halen yeterli olmadığı bilinmektedir. Aslında, en son yayınlanan siber güvenlik politika raporunda *"Amerika'nın büyümekte olan tehditlere karşı kendini koruyabileceği şüphe götürmektedir."* İbaresi yer almaktadır.[18] Hatta raporda daha da ileri gidilerek federal hükümetin giderek büyüyen bu probleme karşı şu anda ve hatta gelecekte de verimli bir şekilde hareket edebilecek bir organizasyona sahip olmadığı ve siber güvenlik ile ilgili sorumlulukların geniş bir federal departman ve kurumlar yelpazesine dağıtıldığı ve bu kuruluşların kendi aralarında birbiriyle ortak düşen sorumluluklarının olduğu ve hiçbirisinin direkt olarak karar verme ve aksiyona geçme yetkisine sahip olmadığının gözlemlendiği açıkça belirtilmiştir.

Bu durumun başlangıç sebeplerini araştırmak için siber açıklıklar ile savaşmak konusunda ortaya konan ilk adımları tekrar gözden geçirmek gerektiği ortaya çıkmıştır. Hükümet, ilk olarak sivil ağın korunması görevini özel sektöre ve federal olarak desteklenmiş CERT/CC gibi kuruluşlara havale etmiştir. Bununla birlikte, istihbarat ve ordu birlikleri ise kendi içlerine kapalı bir savunma mekanizması yürütmüştür. Her ne kadar bu kuruluşların ilk etapta nispeten sahip oldukları teknolojik avantaj onların dış tehditlere karşı üstünlük sağlamalarına sebep olsa da artan teknolojik rekabet ve kuruluşlar arasında işbirliği ve veri paylaşımının olmaması gittikçe büyüyen bir güvenlik ikileminin ortaya çıkmasına sebep olmuştur.

[18] "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

2001 yılındaki olaylardan sonra Amerika, internet güvenlik politikasının tekrar gözden geçirilmesi konusunda kapsamlı bir çalışma başlattı. Bir takım Amerikan başkanı direktifleri aracılığı ile gelişmekte olan DHS (Department of Homeland Security) birimi siber internet güvenliğinin sağlanması için tüm sorumluluğu üzerine almıştır. Bu karar 2003 yılında sunulan "Ulusal Siber Uzay Güvenliğini Sağlama Stratejisi" dokümanında da resmiyete dökülmüş ve siber savunmanın sağlanması açısından iki taraflı bir yaklaşımın ortaya çıkmasına sebep olmuştur. CERT/CC işbirliği ile DHS organizasyonu içerisinde bulunan Ulusal Siber Güvenlik Birimi altında ulusal bir CERT organizasyonu (US-CERT) kurulmuştur. Bu kuruluşun amacı federal sivil ağları (.gov uzantılı) korumak olarak belirlenmiştir. Bir takım federal kurumların çalışmalarını koordine etmek amacıyla DHS'den bir acil çıkış planı ve uyarı sistemi geliştirmesi istenmiş ve ulusal çapta bir siber atağın ortaya çıkması durumunda 19 federal kuruluşun çalışmalarını koordine etme ve yönetme yetkisi verilmiştir. [19]

Yayınlanan bu dokümanda özel sektörün gelişen bir siber tehdide karşılık vermek açısından daha iyi ekipman ve yapıya sahip olduğu vurgulanmış ve ulusal güvenlik birliğinin oluşturulması için ayrıca bir yaklaşımın ortaya çıkarılması konusunun üzeri çizilerek belirtilmiştir. [20] Sonuç olarak, her ne kadar DHS daha önce göz ardı edilmiş bir savunma alanı hakkında sorumluluğu üzerine almış olsa da inter savunma stratejisi konusunun ayrı bir alan olarak belirlenmesi hususunda herhangi bir çalışma ortaya çıkmamıştır.

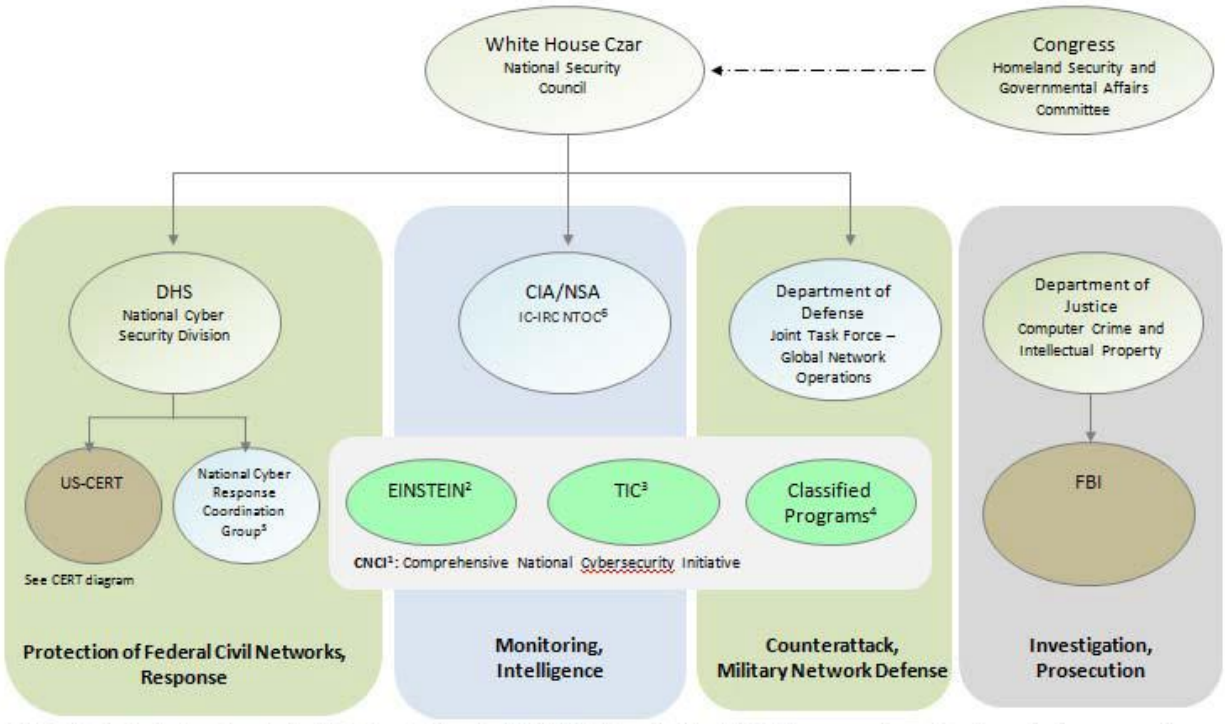
2008 yılında Amerika siber politikası tekrar yenilenerek ve "Kapsamlı Ulusal Siber Güvenlik Girişimi" (Comprehensive National Cybersecurity Initiative, CNCI) başlıklı bir direktif hazırlanarak Başkan Bush tarafından imzalandı. Bu doküman bir takım büyük çaplı politika değişikliklerini içermekteydi. İlk olarak, Yönetim ve Bütçe Ofisi (Office of Management and Budget) DHS'den federal kuruluşlar ve dış sağlayıcılar arasında bulunan ağ bağlantılarının 4 ay içerisinde 4000'den 50'ye düşürülmesini istedi.[21] İkinci aksiyon ise, opsiyonel bir DHS

[19]"The National Strategy to Secure Cyberspace."
http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf
[20]"The National Strategy to Secure Cyberspace."
http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf
[21]Samson, Victoria. "The Murky Waters of the White House's Cybersecurity Plan."*Center for Defense Information*. 23 July 2008.
http://www.cdi.org/program/document.cfm?DocumentID=4345&from_page=../index.cfm

programı olan ve federal web sitelerinden web sitelerine olan internet trafiğini gözlemleyen EINSTEIN adlı programın yetkisinin Ulusal Güvenlik Birimi'ne (National Security Agency) aktarılmasıydı. Bu programın yeni versiyonunda ise trafiğin yanı sıra içeriklerin de yakalanması ve takip edilmesi ve proaktif olarak federal ağların yanı sıra muhtemelen özel ağların da gözlemlenmesi gibi özellikler yer almaktaydı.[22] Son olarak, bu doküman konu hakkında AR-GE yatırım ve çalışmalarının artırılması, siber karşı istihbarat çalışmalarının koordine edilmesi ve hükümet kuruluşları arasında bilgi paylaşımının teşvik edilmesi gibi provizyonları da içermekteydi.[23]

Obama'nın başkanlığında da, var olan CNCI planı desteklenmiş ve çalışmalar hakkında daha fazla şeffaflık olması gerektiği belirtilmiştir. Buna ilaveten, Beyaz Saray yeni bir çalışma ile siber politikasını tamamen revize etmiştir. Oluşturulan son raporda Beyaz Saray içerisinde bir Siber Güvenlik Ofisi'nin kurulması tavsiye edilmiştir. Oluşturulacak bu yapıda bir Siber Çar'ın lider olarak görev alması ve Ulusal Güvenlik Konseyi'nin bir üyesi olması ve Başkan'a kolay ve hızlı erişim ayrıcalığına sahip olması gerektiği belirtilmiştir.[24] Her ne kadar bu ofisin tek başına politika belirleme yetkisi olmasa da, kurumdan federal departmanların çalışmalarını koordine etmesi ve ortak politika belirleme tavsiyelerinde bulunarak federal hükümet içerisindeki tüm siber güvenlik ile ilgili aktiviteler hakkında yetki, rol ve sorumlulukların netleştirilmesinde yardımcı olarak oluşan iletişim ve politika açığı için bir köprü görevi görmesi istenmiştir.[25] Geçmişte yaşanan siber vakalarda ortak bir federal tepkinin olmadığı fark edilerek, kuruluşlar arasında var olan ortak sorumluluk alanlarının ortadan kaldırılması ve hükümet ağı içerisinde siber savunma ile ilgili spesifik rol ve sorumlulukların belirlenmesi tavsiye edilmiştir.

[22]Samson, Victoria. "The Murky Waters of the White House's Cybersecurity Plan."*Center for Defense Information*. 23 July 2008.
http://www.cdi.org/program/document.cfm?DocumentID=4345&from_page=../index.cfm
[23]The Comprehensive National Cybersecurity Initiative.
http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
[24]Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure."
[25]Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure."



1. **CNCI**: Authorized by President Bush via *Presidential Directive HSPD-23*. CNCI is a classified $17 billion program devoted to improving internet security throughout federal and military networks.
2. **EINSTEIN**: Originally an optional program developed by DHS/US-CERT to monitor federal network intrusion, EINSTEIN is now a classified NSA program devoted to monitoring various internet networks, including the private sector.
3. **Trusted Internet Connections Program:** Devoted to reducing the number of connections to Federal networks from 3000 to 50. Co-sponsored by the OMB.
4. The Department of Defense components of the CNCI program remain classified. It is speculated that they include counteroffensive capability.
5. **NCRG**: The National Cyber Response Coordination Group coordinates the efforts of 19+ Federal agencies in the event of an attack of national significance.
6. **IC-IRC:** Intelligence Community—Incident Response Center, **NTOC:** NSA/CSS Threat Operations Center

Yukarıda tavsiye edilen organizasyon şeması yer almaktadır. Bu şemaya bakıldığında Beyaz Saray'da görevlendirilen ve Ulusal Güvenlik Konseyi üyesi olan ve kongreye bağlı olarak çalışan bir Çar başkanlığında 4 ana iş kavramı altında federal kuruluşların birbirleriyle olan bağlantıları resmedilmeye çalışılmıştır.

Federal Sivil Ağların Korunması ve Tepki Konması süreci içinde DHS içerisinde yer alan Ulusal Siber Güvenlik Biriminin (National Cyber Security Division) liderliğinde US-CERT ve Ulusal Siber Tepki Koordinasyon Grubu (National Cyber Response Coordination Group) gibi kuruluşların çalışması öngörülmüştür. Ulusal Siber Tepki Koordinasyon Grubu ulusal çapta etki yaratabilecek bir siber saldırı durumunda 19'dan fazla federal kuruluş arasında koordinasyonun sağlanması ile görevlidir. US-CERT (United States Computer Emergency

Readiness Team) ise daha önce var olan CERT/CC (Computer Emergency Readiness Team Coordination Center) yerine görevlendirilmiştir.

İzleme ve İstihbarat sürecinde ise Merkezi İstihbarat Ajansı (Cetral Intelligence Agency, CIA) ve Ulusal Güvenlik Ajansı (National Security Agency, NSA) işbirliği altında İstihbarat Toplumu-Vaka Tepki Merkezi (Intelligence Community-Incident Response Center, IC-IRC) ve Ulusal Güvenlik Kuruluşu Tehdit Operasyonları Merkezi(NSA/CSS Threat Operations Center, NTOC) gibi kuruluşlar görev almaktadır.

Karşı atak ve Ordu Ağı Savunması sürecinde ise Savunma Departmanı'na bağlı (Department of Defense) Birleşik İş Gücü – Global Ağ Operasyonları (Joint Task Force – Global Network Operasyonları) başkanlığında çalışmalar yürütülmektedir.

Soruşturma ve adli takibat sürecinde ise Adalet Departmanı'na (Department of Justice) bağlı Bilgisayar Suçları ve Fikri Mülkiyetler kuruluşu liderliğinde (Computer Crime and Intelligence Property) Federal İstihbarat Bürosu (Federal Bureau of Intelligence) tarafından çalışmalar yürütülmektedir.

Bunlara ek olarak yukarıda belirtilen ilk 3 süreç için ortak olarak kullanılan EINSTEIN, TIC ve Classified Programs gibi bazı programlar yer almaktadır. EINSTEIN, NSA tarafında kullanılan ve özel ağlar dahil olmak üzere internet ağlarının takip edilmesine yardımcı olan gizli bir programdır. Güvenilir Internet Bağlantıları Programı (Trusted Internet Connections Program, TIC) ise, federal ağ içerisinde bulunan 4000 bağlantının 50'ye düşürülmesinde kullanılan programdır. Üçüncü olarak, Gizli Programlar (Classified Programs) adı altındaki programlar da Savunma Departmanı (Department of Defense) tarafından yürütülen ve karşı taarruz ile ilgili teknolojiyi içerdiği varsayılan programlardır.

Hukuki anlamda organizasyonel yeniden yapılandırma çalışmalarının en önemli örneklerinden bir tanesi 2001 yılında gerçekleşti ve FBI, Ulusal Beyaz Yaka Suç Merkezi (National White Collar Crime Center) ile işbirliğinde bulunarak İnternet Suçu Şikâyet Merkezini (Internet Crime Complaint Center) kurdu. Daha önce INTERPOL tarafından oluşturulan 24/7 ağıyla benzerlikler içermesiyle birlikte IC3 internet suçlarının raporlanması açısında merkezi bir kontak noktası oluşturması amacıyla kurulmuştu. Bu program halen

kullanılmakta olup ülke çapında önemli bir başarıya sahip olmuştur. Yalnızca 2008 yılında sisteme düşen şikâyet sayısı 275.000'i geçmiş ve bu şikâyetlerin %26'sı doğrulanmış ve ilgili hukuki yaptırım kuruluşlarına aktarılmıştır.[26] Öte yandan, her ne kadar bu çalışma ülke açısında büyük bir başarı simgesi olarak kabul edilse de siber suçların önüne geçilmesinde etkin olmamıştır. FBI anketlerine göre halen internet suçlarının büyük bir bölümü daha önceden tespit edilememiş olmakla beraber toplam gerçekleşen vakaların çok küçük bir bölümü IC3 tarafından tespit edilmiştir.

Her ne kadar FBI ve DOJ (Department of Justice)'in çalışmaları ulusal anlamda siber suçlarla savaşmak üzerine odaklanmış olsa da yakın zamandaki bazı çalışmalar ile siber suçlarla ortaya çıkan problemleri önlemek amacıyla yerel kuruluşlara siber suç uzmanları yerleştirilmiştir. Örneğin, 2003 yılında FBI, Bilgisayar Suçları Görev Kuvvetleri (Computer Crime Task Forces) adı altında bir organizasyon kurarak polis kuruluşlarına lokal bilgisayar suçlarının soruşturulması sırasında yardım etmektedir. Şu anda Amerika'da 92 civarında bu anlamda çalışan görev kuvveti yer almaktadır.[27] Aynı sebepten yola çıkarak, Adalet Departmanı (Department of Justice), Bilgisayar Hackleme ve Fikri Mülkiyet (Computer Hacking & Intellectual Property) adı altında yerel federal mahkemelerde yer alan ve siber suçların verimli bir şekilde anlaşılması ve gerekli adli takibatın yapılması konusunda avukatlara eğitim veren birimler kurmuştur.

Federal Ticaret Komisyonu (Federal Trade Commission) siber suçların artmasını önlemede aktif bir rol oynamıştır. Her ne kadar bu çalışma spesifik olarak komisyondan istenmemiş olsa da, FTC'nin tüketici haklarını korumasıyla ilgili çalışmalarının yan ürünü olarak ortaya çıkan bu durum FTC'nin şüpheli hosting sağlayan ve yasadışı aktivitelerin yürütülmesine izin veren internet servis sağlayıcıları hakkında resmi şikâyet duyurusunda bulunma ve gerektiği yerde sınırlandırıcı uygulamada bulunmasına da sebep olmuştur. Bu yüzden FTC, STK, CERT ve yerel hükümet kuruluşlarından gelen zaman duyarlı güvenlik uyarılarına hukuki olarak karşı tepki koyma yetkisine sahip olmasından dolayı sektörler arası işbirliğinin oluşmasında da kritik bir rol üstlenmiştir.

[26] "2008 IC3 Annual Report." http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf
[27] "Netting Cyber Criminals." http://www.fbi.gov/page2/jan06/ccctf012506.htm

ÇİN

Çin Askeri Stratejisi'nde siber güvenlik, Çin Halk Kurtuluş Ordusu'nun (Peoples Liberation Army – PLA) üzerine çok büyük yatırımlar ve çalışmalar yapması gereken çok önemli bir alan olarak tanımlanmıştır.[28] Çinli askeri stratejistlere göre siber güçler, savaş konseptinde güçlü asimetrik fırsatları da beraberinde getirmektedir.[29] Çin Halk Cumhuriyeti, siyasi organizasyonu ve ideolojisi sebebiyle ülkenin güvenliği yanında siber güvenliği de büyük oranda ordunun denetimine bırakmış durumdadır. PLA'nın GSD (General Staff Department) 3. ve 4. Departmanları, ülkenin bilişim altyapısının korunmasından sorumludurlar. Bu birimler hava, kara, deniz kuvvetleri ve milis kuvvetlerin ilgili siber güvenlik birimleriyle birlikte Çin sınırları içerisindeki tüm iletişim trafiğini izlemektedirler.[30] PLA GSD 3. Departmanı ayrıca, Çin ordusunun sahip olduğu bilişim altyapısının ve ağların da güvenliğinden sorumludur. 3. Departman altında 12 adet operasyonel büro vardır. Bunun yanında 3 adet araştırma enstitüsü de ülkenin siber güvenliğinin geliştirilmesi amacıyla aralıksız AR&GE faaliyetleri yürütmekte ve Çin'in önde gelen üniversitelerinin de desteği alınmaktadır. Resmi olmayan bir rapora göre, PLA GSD'ye bağlı 3. Departman bünyesinde 130.000 civarında personel görev almaktadır.[31]

PLA bünyesinde dünyadaki en hızlı süper bilgisayar sistemlerinden bazıları bulunmaktadır. Jiangnan Bilgisayar Teknolojileri Araştırma Enstitüsü (Jiangnan Computer Technology Research Institute) adıyla da bilinen 56. Araştırma Enstitüsü Çin'deki en eski ve büyük araştırma ve geliştirme organizasyonudur. Çok önemli süper bilgisayar yatırımları yapmakta

[28] Chen Zhou, "A Review of China's Military Strategy," China Armed Forces 1:1 (2009): 19.

[29] James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," 257

[30] Roger Faligot, Secret History of Chinese Spies: Chapter 12: The People's Liberation Army of Cyberwarriors (Paris: Nouveau Monde Editions), http://www.lerenseignement.com/nouveaumonde/pdf/4200_Les-services-secrets-chinois---versionanglai.pdf.

[31] Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure, Project 2049 Institute, November 11, 2011 http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

ve bu süper bilgisayarlarla Çin'deki diğer bilgisayar merkezlerine ve PLA bünyesindeki organizasyonlara destek vermektedir. Burada yer alan süper bilgisayarlar sayesinde, diğer ülkelerin kullandıkları karmaşık kodları ve şifreleri kırma çalışmaları hızlanmıştır.[32]

Her ne kadar Çin, bazı batılı ülkeler için ticari espiyonaj ve siber saldırılar konusunda tehdit olarak kabul edilse ve siber suçlular için devlet desteği sağlayan bir ülke olarak adlandırılsa da, siber güvenliğini iyileştirmek ve bunun için gerekli tedbirleri almak amacıyla birçok adım atmıştır. Kaspersky'nin 2010 birinci çeyrek raporunda, 2009'un dördüncü çeyreğinden bu yana .cn uzantılı üst seviye domainlerden kaynaklı kötü niyetli yazılım yüzdesinin %32,8'den %12,84'e düştüğü saptanmıştır.

Bunun temel sebeplerinden birisi ise Çin'in .cn domainler üzerindeki yeni kısıtlamalarıdır. Bu kısıtlamaya göre, .cn uzantılı bir adresi satın almak için hükümet veri tabanında kayıtlı bir işletme ve başvuru sırasında işletme lisansı ve devlet kimlik numarası gösterilmesi gerekmektedir. Çinli operatörlerin genellikle büyük çaptaki siber saldırılara sebep olduğu iddia edilmektedir. Çin Devleti'nin bu iddiaya yanıtı ise, aslında Çin Devleti'nin de sürekli saldırı altında olması ve bu saldırıların genellikle başka ülkelerdeki girişimciler tarafından yapılıyor olmasıdır.[33]

Çin Komünist Partisi'nin resmi gazetesine göre, Çin hükümeti hackleme suçlarının mahkemeler tarafından nasıl değerlendirildiği konusunda sıkı yaptırımlar getirmek için çalışmaktadır. Çin ayrıca online bilgi güvenliği ve siber suçların azaltılması gibi konulardaki hukuki yaptırımlarda değişiklikler yapılmasını önermiştir. 2010 yılında Çin, kullanıcıları siber veri hırsızlığı hakkında korumak amaçlı regülasyonlar getirmiş ve Çinli telekom şebekesi operatörü şirketlerin botnet'lere karşı savaşması ve domain alanları kaydı sırasında sahte isim veya kimlik kullanılmasını önlemek amaçlı ek regülasyonlar yürürlüğe koymuştur.[34]

[32]For example, the 56th Research Institute may be linked with the National Information Assurance
[33]Moore, H. (2010, June 11). *China taking noteworthy steps to improve cybersecurity.*Retrieved June 16, 2010, from The Last Watchdog:http://lastwatchdog.com/china-noteworthy-steps-improve-cybersecurity/
[34]*Fletcher, O. (2010, February 2). China takes step to toughen hacking laws. Retrieved June 16, 2010, from Computer World: http://www.computerworld.com/s/article/9150718/China_takes_step_to_toughen_hacking_laws*

Çin, bunun yanında siber suçlara karşı farkındalığın oluşturulması ve gerekli hukuki takiplerin yapılması için çalışmalarda bulunmuştur. Öte yandan, Çinli güvenlik araştırmacılarının Çin'deki güvenlik şirketlerinde çalışmaya başlamaları Çinli hacker'ların devlet sponsorluğunda çalıştığı iddialarını ortaya çıkarmıştır fakat işin gerçek boyutu Çinli araştırmacıların hükümet için çalışarak kariyerlerini yasallaştırmak istemeleridir. Çin'deki güvenlik endüstrisi halen başlangıç safhalarında olmakla beraber, birçok hacker kendilerine yasal yollardan iş bulamadıklarından dolayı bu tarz suçlar işleyerek para kazanmaya çalışmaktadır. Getirilen yeni kanunlar bu yeni jenerasyon hacker'ları hedef almış ve 2009 yılında uygulanan yeni bir kanun ile hackleme araçlarının dağıtım ve paylaşımı suç olarak kabul edilmiştir.[35]

Çin, bilgi ve siber savaş alanlarında lider konuma gelme hedefini açık olarak beyan etmiş ve bu konular hakkında 20 yıldan bu yana teoriler, doktrinler ve politikalar yayınlamaktadır. 1990'ların ortasından bu yana Çin ordusu "bilgileştirme" konsepti altında modernleşme programı uygulayarak bilgi teknolojileri ve siber uzay alanlarında etkin güç haline gelmeyi planlamaktadır.[36] Ayrıca, Çin'deki bazı ordu eğitim merkezleri siber savaş eğitimleri vermektedir.[37]

Öte yandan Çin, pornografi ve kötü anlamda etkileyici sitelerin yasaklanması amacıyla çok geniş kapsamlı bir sansürleme sistemi yürütmektedir. Çin hükümetinin Bilişim Ofisi Başkanı olan Wang Chen'e göre Çin hükümeti, yakın bir zamanda online kumar, sahtekârlık ve ülkedeki komünist rejimi aşağılayıcı eylemlerde bulunan sitelerin durdurulması için uluslararası kaynaklı online bilgiler hakkında çok sıkı önlemler ve yaptırımlar uygulamaya başlayacaktır. Yakın bir zamanda Çin, telekomünikasyon ve internet hizmeti sağlayıcı şirketlere devlet sırlarını paylaşan kullanıcıların kimliğini bildirmeleri gerekliliğini getiren

[35]Moore, H. (2010, June 11). *China taking noteworthy steps to improve cybersecurity.*Retrieved June 16, 2010, from The Last Watchdog:http://lastwatchdog.com/china-noteworthy-steps-improve-cybersecurity/
[36]Ventre, D. (2010, May 18). *China's Strategy for Information Warfare: A Focus on Energy.* Retrieved June 16, 2010, from Journal of EnergySecurity: http://www.ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinesecyber-threats&catid=106:energysecuritycontent0510&Itemid=361
[37]Ventre, D. (2010, May 18). *China's Strategy for Information Warfare: A Focus on Energy.* Retrieved June 16, 2010, from Journal of Energy Security: http://www.ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinesecyber- threats&catid=106:energysecuritycontent0510&Itemid=361

kanun üzerinde sıkılaştırmalar getirmiş ve bir web sitesi çalıştırmak isteyen herhangi bir kişinin regülatör ile yüz yüze görüşmesi ve fotoğraflarını paylaşmasını zorunlu kılmıştır.[38]

Çin hükümeti ayrıca "Altın Kalkan" adlı, politik anlamda hassas verilerin ülke dışına çıkması veya içeri girmesini önleyen meşhur bir filtreleme sistemi uygulamaktadır. Batıda bu filtre "Büyük Çin Firewall" u olarak adlandırılmaktadır. Bu Altın Kalkan gelecekte bir siber savaş çıkması durumunda Çin'e avantaj sağlayabilecek düzeyde gelişmiş yeteneklere sahiptir.

[38]China Targets 'Foreign Forces' in Web Crackdown. (2010, May 4). Retrieved June 16, 2010, from NewsFactor.com:http://www.newsfactor.com/story.xhtml?story_id=73102

ESTONYA

2007'de Estonya'ya yönelik gerçekleştirilen siber saldırılar, ülkenin siber yeteneklerini ve politikalarını ciddi şekilde sorgulamasına neden olmuştur. Olaylar neticesinde Estonya'da siber savunma faaliyetleri Savunma Bakanlığı gözetiminde gerçekleştirilmektedir.

Bunun yanı sıra, ülkede **Defence League** (Savunma Ligi) adı verilen bir organizasyon da, ülkenin siber savunma yeteneklerini geliştirmek için çalışmalarda bulunmaktadır.[39] Defence League'e bağlı olarak çalışan **Cyber Security Alliance**, 3 ana başlıkta görevlerini icra etmekle sorumludur. Bu görevler;

- Estonyalıların elektronik yaşamlarını koruma altına alma,
- IT uzmanları yetiştirme,
- Siber Savunma hakkında halkı bilgilendirme faaliyetlerinde bulunma olarak sıralanabilir.

a) Belirlenen siber güvenlik politikalarının uygulanabilmesi için oluşturulan Kamu kurumları ve STK'lar, kurumlar arası ilişkiler, özel sektör ve Kamu kurumları arasındaki ilişkiler

Ülkenin Siber Savunma stratejileri, 2007 olayından sonra **Cyber Security Strategy Committee** (Siber Güvenlik Strateji Komitesi) adı verilen bir oluşum tarafından hazırlanmıştır. Komite başkanlığı ve yürütücülüğü Savunma Bakanlığı tarafından yapılmakla birlikte, Dışişleri Bakanlığı, İçişleri Bakanlığı, Eğitim ve Araştırma Bakanlığı, Adalet Bakanlığı ve Ekonomi Bakanlığı da komisyon üyeleri arasında yer almaktadır. Bu komitenin faaliyetleri neticesinde alınan kararlar, bu komiteye bağlı olarak oluşturulan Siber Güvenlik Konseyi tarafından uygulanmaktadır.

Siber Dünya'da Estonya'nın zaaflarını gidermeye yönelik faaliyetlerin temel amacı, ülkenin siber saldırılara karşı savunma yapabilmesini sağlamak ve kritik altyapılara yönelik atakların

[39] Estonia Ministry of Defense, Cyber Security Strategy Committee, Cyber Security Strategy, Talin 2008

en kısa sürede çözüme kavuşturularak etkisini minimize etmek olarak belirtilebilir. Bu hedeflerden yola çıkarak ülkenin; güvenlik ölçütlerinde çok katmanlı yapıya geçmesi, bilişim güvenliğinde uzmanlığını geliştirmesi, siber güvenliği geliştirecek yönetsel reformlara imza atması ve uluslararası işbirliğini artırmaya çalışması ilkelerini benimsediği söylenebilir.

Estonya, üyesi olduğu NATO çatısı altında Bilişim Güvenliği alanında uluslararası işbirliğinin önemini gören ve bu alanda aktif rol alan ülkelerden biridir. Bu işbirliği, kendi savunma yetkinliğinin artmasının yanı sıra NATO üyesi diğer ülkelere de önemli katkılarda bulunmasını sağlamaktadır. Bir NATO kuruluşu olarak 2008 yılında Tallinn kentinde faaliyete geçen **Cyber Defence Centre of Excellence** (Siber Savunma Mükemmeliyet Merkezi), üye ülkeler arasında işbirliğini artırma, bilgi paylaşımı sağlama ve siber güvenlik alanında araştırmalar yapma hedefine yönelik faaliyetlerde bulunmaktadır.[40] Merkezin destekçileri olan ülkeler; Estonya, Almanya, Macaristan, İtalya, Letonya, Litvanya, Slovakya ve İspanya olarak sıralanabilir.

Estonya, kurmuş olduğu **Department of Critical Infrastructure Protection** (Kritik Altyapıları Koruma Şubesi) ile stratejik öneme sahip genel ve özel ağlarını koruma altına almaya çalışmaktadır. Bu merkezde risk değerlendirme, kritik altyapılara yönelik bilgi toplama ve siber tehditlere karşı saldırı mekanizmaları oluşturarak riskleri bertaraf etmeye yönelik çalışmalar yapılmaktadır. Gerçekleştirilen projeler arasında, kritik altyapılara yönelik döküm çalışması yapma, acil eylem planları geliştirme ve geniş çaplı siber ataklara karşı risk değerlendirme faaliyetlerini raporlama bulunmaktadır.

b) İlgili kurumların görevlendirmelerine dayanak olan hukuki mevzuatlar, kurumların görev ve yetki sınırlarının çerçevesi

Estonya'nın siber güvenlik konusunda oluşturmaya çalıştığı hukuki altyapı ve mevzuatlar, temel olarak 3 hedefi gözetmektedir. Bunlar;

- Estonya'nın kabul ettiği Siber Güvenlik Stratejisi'ne uyum sağlayan ve bu stratejik hedefler için ihtiyaç duyulan kanuni değişikliklerin yapılması

[40] NATO Center for Strategic and International Studies, Preliminary Assessment of National Doctrine and Organization, Cybersecurity and Cyberwarfare, 2011

- Kritik bilgi altyapılarının korunmasına yönelik mevzuatların hazırlanması ve yürürlüğe konması,
- Estonya'da geliştirilen ve düzenlenen mevzuatların, uluslararası platformda ve özellikle AB üye ülkelerinde tanıtılması, benzer mevzuatların bu ülkelerde yapılmasının sağlanmasıdır.

Çalışmaların en başında ülkenin genel durumu incelenmiş, Siber Güvenlik Stratejisine uyumlu olan ve olmayan, ihtiyaç duyulan ve çalışmaları engelleyen kanun ve yönetmelikler tespit edilmiştir. Bu çalışmaların sonunda görülmüştür ki, Estonya'da hali hazırda yürürlükte olan yönetmelikler, merkezileştirilmeyen ve hatta birbiriyle çakışan hükümler içermektedir. Örnek vermek gerekirse, yürürlükte olan ve elektronik servislerin daha liberal ve serbestçe kullanılmasını yaygınlaştırmaya yönelik mevzuatlar bulunmasına rağmen yürürlükte olan bir diğer mevzuat kişisel veri koruması hükümlerinin oldukça kapalı ve sıkı şekilde denetlenmesini salık vermektedir.

Yapılan incelemelerde görülmüştür ki, ihtiyaç duyulan hukuki altyapı belirli konularda net hükümler içermelidir. Bu başlıklar ise aşağıdaki gibi tespit edilmiştir:

Ceza Kanunu

Gerçekleştirilmiş olan siber suç faaliyetlerini kapsamlı şekilde cezalandıran yasaların eksikliği göze çarpmaktadır. Özellikle terör faaliyetlerini destekleme amacıyla yapılmış olan siber saldırılara karşı özel hukuki düzenlemelerin yapılmamış olması büyük bir eksiklik olarak göze çarpmaktadır.

Elektronik Haberleşme Kanunu

Bu kanun, vatandaşların elektronik haberleşme teknolojilerinden faydalanırken paylaşmış bulundukları ve kendi veri güvenliklerini tehdit edebilecek hassasiyette, bilişim teknolojileri çözümlerinde (sunucu, veri tabanı gibi) tutulan verilerin güvenliğini tahsis etmek amacıyla hazırlanmıştır. Son kullanıcıların bu konulardaki aczinin de düşünülerek hazırlandığı mevzuatta, kişisel verilere 3. şahısların erişiminin önü alınmış ve hangi durumlarda bu verilere erişilebileceği net şekilde belirlenmiştir.

Kişisel Verilerin Koruması Kanunu

Bu kanun siber güvenlik alanında yürütülecek resmi faaliyetlerde kişisel verilere hangi kurumların hangi şartlar ve izinlerle erişebileceğini denetler. Bu kanunla birlikte, kişisel verilere erişimin fiziksel, teknik ve organizasyonel ölçütlerle tespiti yapılmış; kullanışlılık, bütüncüllük ve güvenilirlik perspektiflerinde değerlendirmelerde bulunulmuştur.

Örnek vermek gerekirse, ulusal güvenliğin tehdit altında olduğu durumlarda, daha önceden yetkilendirilmiş birimlerin her türlü veriye en hızlı şekilde nasıl erişebileceğinin tanımı da bu kanunda yer almaktadır. Tahmin edilenin aksine kişisel verilerin sadece korunması değil, ihtiyaç halinde yetkili birimlerin bu verilere en hızlı nasıl erişebileceğinin tanımı da bu kanun kapsamında değerlendirilmiştir. Bu tarz özel imtiyazlar, Avrupa Birliği'nin 95/46/EC direktifiyle desteklenmiş olan Avrupa Konseyi'nin ETS 108. kararıyla netleştirilmiştir.

Böyle özel imtiyazların tanınması bu yetkiyle işlem yapacak olan görevlilerin suistimali ihtimali nedeniyle tartışma konusu olsa da, kritik altyapılar ve ulusal güvenliğin tehdit altında olduğu dönemlerde, mesela bir siber savaşta başvurulması gereken bir çözüm olması nedeniyle üzerinde anlaşmaya varılmıştır.

Bu nedenle Adalet Bakanlığı ile birlikte sıkı bir çalışma içerisine girilmiş ve atılacak adımlar görüş alışverişinde bulunarak net şekilde tespit edilmiştir. Çıkarılacak mevzuatlar açısından Siber Güvenlik Komisyonunun böyle bir dirsek teması içinde bulunması kaçınılmaz olmuştur.

Bu ve buna benzer kanunlarla siber tehditlere karşı alınacak tedbirler, siber güvenliğin tesisine yönelik gerçekleştirilecek çalışmalar ve oluşturulacak çalışma gruplarının belirlenmesiyle birlikte hangi mevzuatları referans alarak bu yetkiyi kullanacaklarına dair tespitler yapılmıştır.

Estonya, yaşadığı acı tecrübeden dersler çıkarmış ve tehdidin büyüklüğünü fark etmiştir. Birçok ülkeden daha hızlı bir şekilde ihtiyaç duyduğu çalışma gruplarını oluşturmuş, gerekli mevzuat değişikliklerini yaparak bu çalışma gruplarını kanuni güvence altına almış ve yetkilendirmiş, olası tehditlere karşı senaryoları canlı tutarak gerçek bir saldırı anında alacağı aksiyonları belirlemiştir.

Bu bakış açısıyla Estonya'nın siber güvenliğin tesisi açısından referans ülke olarak değerlendirilmesi ve gerçekleştirdiği reformların irdelenmesi ülkemiz açısından da faydalı olacaktır.

FRANSA

İnternet kullanıcılarıyla ilgili güvenlik tedbirlerinin yanı sıra, Fransa son yıllarda savunma ve ulusal güvenlik politikalarını da ciddi bir biçimde gözden geçirmiştir. Buna uygun olarak konuyla ilgili yeni öncelikler tespit edilmiş ve bu öncelikler Fransa Cumhurbaşkanı Nicolas Sarkozy tarafından 2008 yılında bir rapor halinde onaylanmıştır.[41] Bu raporda toplumun iletişim teknolojilerine artarak süren bağımlılığı göz önünde bulundurularak siber saldırılar en önemli milli güvenlik sorunlarından biri olarak tanımlanmıştır. Ayrıca raporda siber alan da Fransız egemenlik alanı içerisinde tanımlamış ve bu alanda savunma ve saldırı kabiliyetini arttırıcı stratejiler oluşturmuştur.

Fransa'da siber güvenlik ile ilgili temel kurum 2009 yılında kurulan Ulusal Bilgi Sistemleri Güvenlik Ajansı'dır. Bu kurumun görev alanları arasında siber saldırıları tespit ve karşı cevap, araştırma ve geliştirme faaliyetleri vasıtasıyla siber saldırıların önlenmesi ve hükümete ile kritik önemi haiz kurumlara bilgi sağlamak bulunmaktadır.[42] Bu kurum doğrudan Başbakana bağlı olarak Milli Güvenlik Genel Sekreterliği gözetimi altında faaliyetlerini yürütmektedir. Siber güvenliğin yanı sıra Fransa, ayrıca uzmanlaşmış kurumlar bünyesinde siber saldırı kabiliyetlerini de geliştirmektedir.[43] Hem kara kuvvetleri hem de hava kuvvetleri bünyesinde elektronik saldırı üniteleri bulunmaktadır.[44] Ayrıca Fransız istihbarat teşkilatı da siber saldırı unsurlarını yakından takip etmektedir.[45]

Şubat 2011'de, Ulusal Bilgi Sistemleri Güvenlik Ajansı bilgi sistemlerinin savunması ve güvenliğiyle ilgili ulusal strateji planını yayınlamıştır. Mezkûr strateji temel olarak 4 ana prensibi içermektedir:

1- Siber güvenlik alanında uluslararası bir güç konumuna erişmek,

[41]"The French White Paper on Defence and National Security", 2008, <www.ambafranceca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf>.
[42]"France Country Report", European Network and Information Security Agency, 2010, <www.enisa.europa.eu/act/sr/files/country-reports/France.pdf>, pp. 5, 23.
[43]"The French White Paper on Defence and National Security", 2008, <www.ambafranceca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf>, p. 3.
[44]"Chapter Four: Europe", *The Military Balance*, vol. 111, no. 1, 2011, pp. 104–09.
[45]"French White Paper on Defence and National Security", 2008, <www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf>, p. 9.

2- Bilgi egemenliğini temin etmek suretiyle Fransa'nın karar alma inisiyatifini korumak, (Burada özellikle kritik kararlar almak durumunda olan hükümet yetkililerinin birbiriyle iletişimlerinin gizliliğinin temin edilmesi amaçlanmaktadır.)
3- Kritik önemi haiz ulusal altyapıların siber güvenliğinin temin edilmesi
4- Siber ortamda gizliliğin ve güvenliğin sağlanmasıdır.[46]

Fransa yukarıda belirtilen amaçlara ulaşmak için aşağıdaki uygulamaların hayata geçirilmesi gerekliliğini kararlaştırmıştır. Bu uygulamalar;

1- Sağlıklı kararlar almak için güvenliği temin edilecek ortamın iyi araştırılması,
2- Saldırıları tespit edip onlara karşılık verilmesi, zarar görmesi muhtemel kişilerin uyarılması ve onlara yardım edilmesi,
3- Siber özerkliğin sağlanması için Fransa'nın; ilmi, teknik, endüstriyel ve beşeri becerilerinin arttırılıp devam ettirilmesi,
4- Devletin ve kritik altyapı hizmetini sunan hizmet sunucularının bilgi sistemlerinin güvenliğinin temin edilmesi,
5- Kuralların teknolojideki yeniliklere uyum sağlayabilecek nitelikte düzenlenmesi,
6- Bilgi sistemlerinin güvenliği, siber suçlarla mücadele ve siber güvenlik hususlarında Fransa'nın uluslararası işbirliklerinin geliştirilmesi, (Bu amaçla Almanya ve Amerika Birleşik Devletleri ile özel olarak anlaşma imzalanmış, ayrıca AB ve NATO bünyesinde de uluslararası işbirliği yapılmıştır.)
7- Fransa'da yaşayan bireylerin bilgi sistemi güvenliğiyle ilgili hususları daha iyi kavrayabilmesi adına bunların düzenli olarak bilgilendirilip, konuyla ilgili ikna olmalarının sağlanmasıdır.[47]

Fransa'da konuyla ilgili hukuki düzenlemeler temel olarak şunlardır:

- E-Devlet Kanunu,
- 8 Kasım 2005 tarihli Kamu Kurumları ile Bireyler ve Kamu Kurumları arasındaki Elektronik Etkileşime dair Yönetmelik,

[46] *Défense et sécurité des systèmes d'informations: Stratégie de la France*, National Network and Information Security Agency, 2011.
[47] "France Country Report", European Network and Information Security Agency, 2010, <www.enisa.europa.eu/act/sr/files/country-reports/France.pdf>, p.6.

- 6 Ocak 1978 tarihli Bilgi Teknolojileri ve Özgürlükler Kanunu -belirtmek gerekir ki bu kanuna göre veri güvenliğinin temini amacıyla Ulusal Enformatik ve Özgürlükler Komisyonu kurulmuştur-
- e-ticaret mevzuatı,
- e-iletişim mevzuatı,
- siber suçlara karşı mücadeleyi amaçlayan 5 Ocak 1988 tarihli Godfrain Kanunu -bu kanun alanında bir ilk olma özelliği taşımaktadır-
- e-kimlik mevzuatıdır.

BİRLEŞİK KRALLIK

Birleşik Krallık hükümeti Ekim 2010'da Ulusal Güvenlik Stratejisi Raporu'nu parlamentoya sunmuş ve yayınlamıştır.[48] Rapor, Birleşik Krallık'ın karşılaşabileceği riskleri gruplara ayırmış ve siber saldırıyı en yüksek risk grubunda değerlendirmiştir. Rapor, siber saldırı kapsamına diğer ülkeler tarafından yönlendirilecek siber saldırıları ve terörist gruplar ile organize şebekeler tarafından yönlendirilecek siber saldırıları da almıştır. Ulusal Güvenlik Stratejisi Raporu, açık bir şekilde, farklı ülkelerin Birleşik Krallık'a siber saldırılar düzenlediğini belirtmekte ve siber güvenliğin, raporun düzenlendiği yıl ve onu izleyen beş yıl boyunca en yüksek dereceli ulusal güvenlik risklerinden biri olarak değerlendirilmesi gerektiğinin altını çizmektedir.

Ulusal Güvenlik Stratejisi ile dört yıllık Ulusal Siber Güvenlik Programı hazırlanmış ve siber güvenlik için 650 milyon poundluk bir bütçe belirlenmiştir. Ulusal Siber Güvenlik Programı ve ayrıntıları, Kasım 2011'de yayınlanan Siber Güvenlik Stratejisi Raporu'nda belirtilmektedir.[49] Ulusal Siber Güvenlik Programı, Kabine Ofisi'ne bağlı olan "Office of Cyber Security and Information Assurance" tarafından yönetilmektedir. Yeni Ulusal Siber Güvenlik Programı ile birlikte, Birleşik Krallık, siber güvenlik alanında köklü değişikliklere gitmiş ve birçok yeni kurumun kurulma çalışmalarına başlamıştır.

Ulusal Siber Güvenlik Programı için ayrılan 650 milyon poundluk bütçenin %59'u "Single Intelligence Account" adındaki Birleşik Krallık'ın üç istihbarat ve güvenlik kuruluşuna (MI6, MI5 ve GCHQ) para sağlayan fona, %14'ü ise Savunma Bakanlığı'na ayrılmıştır.

Değişen Algı ve Değişen Tehditler

Birleşik Krallık siber güvenlik kapsamındaki korumayı üç açıdan değerlendirmekte ve siber güvenlik politikalarını buna göre belirlemektedir. Buna göre, siber saldırılara karşı,

i) hükümet ve devlet kurumları,

[48] A Strong Britain in an Age of Uncertainty: The National Security Strategy, October 2010
[49] The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, November 2011

ii) siber ortamdaki her türlü iş ve işlem ile özel sektör ve

iii) halk korunmalıdır.

Siber Güvenlik Stratejisi raporu, internetin gelişimi ile tehditlerin de değiştiğini belirtmekte ve tehditleri dört gruba ayırmaktadır. Bunlar;

a) Bilişim sistemlerine yönelen ve/veya bilişim sistemlerini kullanan suçlular,
b) Diğer ülkeler,
c) Terörist gruplar,
d) Kamu ve özel sektöre saldırılarda bulunan ve genelde politik amaçlar doğrultusunda hareket eden "Hacktivist" gruplardır.

Askeri ve İstihbarat Alanları

Ulusal Siber Güvenlik Programı ile birlikte, Birleşik Krallık, ülke çapında yeni siber güvenlik birimleri kurma çalışmalarına başlamıştır. Savunma Bakanlığı nezdinde askeri alanda çalışacak iki merkez kurulmaktadır. Bunların ilki, Küresel Operasyonlar ve Güvenlik Kontrol Merkezi (Global Operations and Security Control Centre)'dir. Askeri bir üste kurulan bu merkez silahlı kuvvetler için siber savunma odaklı olarak çalışmaktadır. Bunun yanı sıra "Defence Cyber Operations Group" isminde bir birim kurulmaktadır. Birimin Nisan 2012'de çalışmalara başlaması, Nisan 2014'te ise tam kapasiteye ulaşması planlanmaktadır. Savunma alanında siber savunmayı geliştirmek için çalışacak bu merkeze bağlı "Joint Cyber Unit" isminde bir kuruluş bulunacaktır. Birleşik Krallık'ın üç istihbarat ve güvenlik kuruluşundan biri olan GCHQ'nun arazisinde kurulacak olan bu kuruluş, siber dünyada kullanılacak yeni operasyonel taktik ve teknikler geliştirmek için çalışacaktır.

Birleşik Krallık, ayrıca, askeri alanda savunma teçhizatı alımı konusunda da yeni bir politika geliştirmektedir. Önemli savunma teçhizatlarının alındığı firmalar için getirilen fiziksel güvenlik koşullarının yanı sıra bu firmalar için siber güvenlik koşulları da getirilecek ve bu firmalardan önemli verilerin çalınması engellenmeye çalışılacaktır.

Güvenlik Teşkilatı

Birleşik Krallık' ta organize suçlardan sorumlu olan "Serious Organised Crime Agency" teşkilatı, 2013 yılına kadar yerini "National Crime Agency" isimli teşkilata bırakacaktır. Teşkilatın siber suçlar ile ilgili bir birimi olacak ve ulusal çaptaki büyük siber suçlar ile bu teşkilat ilgilenecektir. Teşkilat ayrıca polis teşkilatına da siber suçlar konusunda destek verecektir. Teşkilat kadrosunda, yalnızca polis ve güvenlik güçlerini değil aynı zamanda farklı siber suç uzmanlarını da barındıracaktır.

İletişim Altyapısı

Kritik altyapılarının büyük bir kısmının özel sektörün elinde olduğunu bilen Birleşik Krallık, Ulusal Altyapının Korunması Merkezi (Center for the Protection of National Infrastructure) aracılığı ile söz konusu özel sektör kuruluşları ile devamlı iletişim halindedir. Merkez, ilgili kuruluşlar ile terörizm, espiyonaj gibi tehditlere karşı siber alanı da içerecek şekilde bilgi alışverişinde bulunmaktadır.

Siber Güvenlik Uzmanlarının Yetiştirilmesi ve Siber Güvenlik Araştırmaları

Ulusal Siber Güvenlik Programı çerçevesinde, Birleşik Krallık, etik hacker yetiştirme çalışmalarına hız vermiştir. Bu kapsamda üniversitelerde konu ile ilgili lisansüstü programlar geliştirilecek, yeni sertifika programları oluşturulacak ve GCHQ'nun yardımı ile siber güvenlik alanında bir araştırma merkezi kurulacaktır. Söz konusu araştırma merkezine 3,5 yıl için 2 milyon poundluk bir bütçe ayrılmıştır.

ALMANYA

Almanya Federal Hükümeti, ülkelerinde sosyal ve ekonomik refahın teşviki amacıyla cyberspace'e büyük bir katkı sağlamayı amaçlamaktadır. Siber Güvenlik Stratejisi ağırlıklı olarak sivil yaklaşımlar ve önlemler üzerinde durmaktadır. Almanya'nın önleyici siber güvenlik stratejisi Alman Ordusu tarafından sağlanmaktadır. Bilgi ve iletişim teknolojilerinin küresel doğası göz önüne alındığında, uluslararası koordinasyon ve ağların dış güvenlik politikalarıyla işbirliği vazgeçilmezdir.

Bu işbirliğine yalnızca Birleşmiş Milletler değil aynı zamanda AB, Avrupa Konseyi, NATO, G8, AGİT ve diğer çok uluslu örgütler de dahildir. Burada amaç uluslararası toplumun siber güvenliğini sağlamak için tutarlı bir ortam oluşturmaktır.

Stratejik Hedefler ve Tedbirler

Mevcut Siber Güvenlik Stratejisi ile Federal Hükümet, CIP ile kurulan yapılar bazında, mevcut tehditlere karşı kurulan uygulama planı ve tedbirlere uyar.

Federal Hükümet, özellikle on stratejik alana odaklanacaktır:

:

1. Kritik Bilgi Altyapıları Korunması

Kritik bilgi altyapılarının korunması, siber güvenliğin öncelikli konusudur. Neredeyse tüm kritik altyapıların merkezi ve bir bileşeni olarak giderek önem kazanmaktadır. Kamu ve özel sektör olarak gelişmiş, stratejik ve organizasyonel bilgi paylaşımı yoğunlaştığı için daha sıkı bir koordinasyon oluşturmak gerekmektedir. Bu amaçla, CIP işbirliği ile kurulan uygulama planı sistematik olarak uzar ve yasal taahhütleri geliştirmek için, CIP uygulama planı bağlayıcı niteliği incelenir. Ulusal Siber Güvenlik Konseyi'nin katılımı ile ek sektörlerin entegrasyonu incelendiğinde, ilgili olan yeni teknolojilere giriş büyük ölçüde kabul edilmektedir. Koruyucu

tedbirler olmak zorundadır. Ek yetki durumunun gerekli olup olmadığı ve belirli tehditlerin açıklığa kavuşturulması gerekir. Ayrıca IT krizleri sırasında, kritik altyapıları korumak için uyum kurallarının gerekliliğini incelemek gerekmektedir.

2. Almanya'da Güvenli IT Sistemleri

Vatandaşlar ve küçük – orta ölçekli işletmeler tarafından kullanılan IT sistemleri için daha fazla güvenlik gerektiren altyapılar oluşturulmalıdır. Kullanıcılar, IT sistemlerinin kullanımı ile ilgili riskler ve güvenlik konusunda uygun ve tutarlı bilgi sahibi olmalıdırlar. Ortak girişimlerle beraber toplumu bilgilendirmek amacıyla bilgi havuzu oluşturulmalı ve birbiriyle tutarlı tavsiyeler devamlı olarak verilmelidir. Ayrıca devlet, bilgi sağlayıcıların sorumluluklarını denetleyerek, kullanıcılara sunulan temel bilginin, uygun güvenlik ürünleri ve hizmetleriyle verildiğinden emin olmalıdır. Devlet, vatandaşların büyük çoğunluğu tarafından kullanılan ve devlet tarafından onaylamış (kimlik veya e-posta örneğin, elektronik kanıt vb.) temel güvenlik işlevleri için özel teşvikler ve fonlar sunmalıdır. IT sistemlerinin güvenli kullanımında küçük ve orta ölçekli işletmelerin desteklenmesi için Ekonomi ve Teknoloji Federal Bakanlığı sanayinin katılımı ile IT güvenliği konusunda bir görev gücü kurmuştur.

3. Kamu Yönetiminde IT Güvenlik Güçlendirilmesi

Kamu yönetiminin IT sistemleri korunması daha da arttırılacaktır. Devlet yetkililerin veri güvenliği konusunda rol model olarak hizmet etmeleri gerekmektedir. Elektronik ses ve veri iletişimi için, bir temel olarak, federal yönetiminde güvenli bir ağ altyapısını (Federal Network gibi) oluşturması gerekmektedir. Almanya hükümeti olarak, federal yönetim için uygulama planı sürdürmeye devam edilmektedir. IT güvenlik durumunun kötüleşmesi halinde, bu plan da oluşan durumlara göre hizalanabilir. Etkili IT güvenliği federal yetkililer tarafından güçlü bir yapılanma gerektirir. Bu nedenle kaynakların, merkezi ve yerel düzeyde uygun olarak dağıtılması gerekir. Federal Hükümetin IT Güvenlik uygulaması, ortak yatırımların uygulanmasını kolaylaştırmak için, yetkililer tarafından tek tip eylem olarak, düzenli bir biçimde bütçe imkânları doğrultusunda yapılacaktır. Federal eyaletlerle operasyonel işbirliği -

özellikle CERTS (Bilgisayar Acil Durum Müdahale Ekipleri) ile- IT Planlama Konseyi tarafından yoğunlaştırılacaktır.

4. Ulusal Siber Müdahale Merkezi

Bütün devlet makamları arasında operasyonel işbirliğinin oluşturulması ve IT olaylarından korunma ve müdahale önlemlerinin koordinasyonunu geliştirmek için bir Ulusal Siber Müdahale Merkezi kurulacaktır. Bu merkez, Bilgi Güvenliği Federal Dairesi, Anayasayı Koruma ve Sivil Koruma Federal Dairesi ve Afet Yardımı Federal Dairesi'ne rapor vererek doğrudan işbirliği yapacaktır. Ulusal Siber Müdahale Merkezi, ilgili tüm makamların yasal görevleri ve yetkilerine, sıkı işbirliği anlaşmaları temelinde uyacaktır. Federal Kriminal Dairesi (BKA), Federal Polis (BPOL), Gümrük Kriminolojik Ofisi (ZKA),Federal İstihbarat Servisi (BND), Alman Ordusu ve kritik altyapı işletmecileri denetleme makamlarının hepsi kendi kanuni görevleri ve yetkileri çerçevesinde bu çatı altında toplanmıştır. IT ürünlerinin zayıflıkları, hassas noktaları, saldırı formları, fail profilleri, hızlı ve yakın bilgi paylaşımı için Ulusal Siber Müdahale Merkezi, IT olaylarının analiz ve eylemleri için birleştirilmiş tavsiyeler vermeyi sağlar. Özel sektörün, siber suçlar ve casusluklara karşı kendini korumak için olan çıkarları ve aynı zamanda sorumlulukları da dikkate almalıdır. Her paydaş ortaklaşa geliştirilen ulusal siber güvenlik değerlendirmesi temelinde, kendi görevi içinde gerekli önlemleri alır ve yetkili makamların yanı sıra sanayi ve akademi ortakları ile koordine eder. Güvenlik hazırlıklarının en iyi elde edilme yöntemi, erken uyarı ve önleme ile olduğundan, Siber Müdahale Merkezi, düzenli olarak ve belirli olaylar için Ulusal Siber Güvenlik Konseyi'ne öneriler sunacaktır. Bir Siber Güvenlik sorununun yakın olması ya da zaten ortaya çıkan Siber Güvenlik sorununun kriz seviyesine ulaşması halinde, Ulusal Siber Müdahale Merkezi, doğrudan İçişleri Federal Bakanlığı'ndan sorumlu Devlet Bakanı başkanlığında olan kriz yönetim kadrosunu bilgilendirecektir.

5.Ulusal Siber Güvenlik Konseyi

Krizlerin yapısal nedenlerinin belirlenmesi ve ortadan kaldırılması, siber güvenlik için önemli bir önleyici araç olarak kabul edilir. Ulusal Siber Güvenlik Konseyi, önleyici araçları ve kamu ve özel sektörün disiplinler arası siber güvenlik yaklaşımlarını koordine etmek için tasarlanmıştır. Ulusal Siber Güvenlik Konseyi'nin amacı; federal, politik ve stratejik düzeyde siber güvenlik alanında, IT Planlama Kurulu iş yönetimini tamamlamak olacaktır. Bu nedenle Federal Hükümet içinde, Federal Hükümet Temsilcisi'nin sorumluluğunda, kamu ve özel sektör arasında Bilgi ve İletişim Teknolojilerinin işbirliği için daha görünür bir Ulusal Siber Güvenlik Konseyi kurmak istenmektedir. Bu konseye Federal Eyaletlerin; her Federal Dışişleri Bakanlığından Federal İdareci ve Genel Sekreter, İçişleri Federal Bakanlığı, Savunma Federal Bakanlığı, Ekonomi ve Teknoloji Federal Bakanlığı, Federal Adalet Bakanlığı, Federal Maliye Bakanlığı, Eğitim Ve Araştırma Federal Bakanlığı'ndan 6 temsilci katılacaktır ve belirli durumlarda ek bakanlıklar sürece dahil edilecektir. İş temsilcileri ortak üye olarak davet edilecektir. Gerekirse akademi temsilcileri de dahil olacaklardır.

6. Siber Uzam (Cyberspace)'date Etkili Suç Kontrolü

Bilgi Güvenliği ve özel sektörün siber suçla mücadelesinde, ayrıca casusluk ve sabotaja karşı koruma konusunda Federal Dairenin ve kolluk kuvvetlerinin yeteneklerini güçlendirilmesi gerekmektedir. Sanayi ile ortak kurumların Know-How değişimini geliştirmek için Almanya Hükümeti, yetkili kolluk kuvvetlerinin katılımı ile bu alanda danışman sıfatıyla hareket edecektir. Siber suçlarla mücadelede, yapısal zayıflıkları olan ortak ülkelere, destek için projelerle destek verilecektir. Avrupa Siber Suçlar Sözleşmesi Konseyi çerçevesinde, artan siber suç faaliyetleriyle yüzleşmek için ceza hukuku açısından küresel uyum sağlamak amacı ileiçin büyük bir çaba harcanmaktadır. Dahası, bu alanda ilave kuralların BM seviyesinde gerekli olup olamayacağı incelenir.

7.Avrupa'da ve Tüm Dünyada Siber Güvenlik Sağlamak İçin Etkili Koordine Eylemleri

Dünya çapında cyberspace güvenliğine sadece milli ve uluslararası düzeyde koordine edilmiş araçlarla ulaşılabilir. Biz Avrupa Birliği düzeyinde, ICT'deki değişmiş tehdit hali ve Avrupa Birliği kurumlarındaki IT yeterliliğinin havuzlaştırılması (pooling) nedeniyle kritik öneme sahip bilgi altyapılarının korunması, Avrupa Ağı ve Bilgi Güvenliği Kurumu'nun (ENISA) direktifinin uzatılması ve genişletilmesi için hareket planına dayanan uygun tedbirleri destekliyoruz. Avrupa Birliği Dahili Güvenlik Stratejisi ve Dijital Gündem ilerideki aktiviteler için rehberlik sağlayacaktır. Harici siber politikamızı, siber güvenliğe ilişkin Alman görüş ve fikirlerinin Birleşmiş Milletler, OSCE, Avrupa Konseyi, OECD ve NATO gibi uluslararası kuruluşlarca izleneceği ve bunlara uyumun sağlanacağı şekilde şekillendireceğiz. İktidarların değerlendirmesi ve karar alma güçlerinin ihtiyacı doğrultusunda giderek daha çok taraflı bir yaklaşım benimsenmelidir. Bu bağlamda mümkün olduğunca fazla ülke tarafından imzalanacak ve güven arttırıcı önlemler ihtiva eden sanal cyber space'te devletin hareketini düzenleyen siber kanun hazırlanmalıdır. G8 çerçevesinde hali hazırda botnet karşıtı faaliyetler güçlendirilmektedir. NATO Atlantik aşırı güvenlik üssü olarak hizmet etmektedir. Bundan dolayı NATO, siber güvenliğin bütün sorumluluklarını göz önünde bulundurmak zorundadır. NATO'nun yeni stratejik konseptinde öngörüldüğü gibi Üye Devletlerin aynı zamanda ihtiyari olarak kritik öneme sahip sivil altyapısında da kullanabileceği birleşik güvenlik standartları oluşturma kararlılığının taraftarı olunmalıdır.

8.Güvenilir Ve Sağlam Bilgi Teknolojileri Kullanımı

Güvenilir IT sistemleri ve bileşenlerinin ulaşılabilirliği devamlı bir şekilde sağlanmalıdır. Sosyal ve ekonomik açıları dikkate alan geliştirilmiş güvenlik için yenilikçi koruma planlarının geliştirilmesi desteklenmektedir.

Bu maksatla IT güvenliği ve kritik altyapı koruması üzerine olan araştırma devam ettirilecek ve güçlendirilecektir. Bundan başka Almanya'nın teknolojik egemenliğini ve temel stratejik IT yetkinliğindeki ekonomik kapasitesi kuvvetlendirilecek, bunlar politik stratejiler kapsamına alınacak ve daha da geliştirilecektir. Ulusal kaynaklar özellikle Avrupa'daki müttefiklerle ve

ortaklarla rasyonel durumlarda bir araya getirilecektir. Teknolojik çeşitlilik taraftarı olarak amaç; bileşenleri, uluslararası tanınmış sertifikasyon standartları tarafından onaylanmış kritik güvenlik alanlarında kullanmaktır.

9. Federal Makam ve Mercilerde Personel Gelişimi

Siber güvenliğin stratejik önemi nazara alındığında yetkili makam ve mercilerde siber güvenlik için ilave kadronun gerekli olup olmadığı bir öncelik olarak incelenmelidir. Dahası federal makam ve merciler arasındaki personel değişiminin yoğunlaştırılması ve uygun ilave eğitim tedbirleri bakanlıklar arası yardımlaşmayı arttıracaktır.

10. Siber Saldırılara Cevap Vermek İçin Araçlar

Eğer devlet siber saldırılara karşı tamamıyla hazırlıklı olmak istiyorsa siber saldırılara cevap vermek için koordineli ve kapsamlı bir araçlar bütünü yetkili devlet makam ve mercilerinin işbirliği ile oluşturulmalıdır. Düzenli olarak tehdit durumunu değerlendirilerek gerekli koruma önlemlerini alınmalıdır. Gerekli olması halinde, federal veya Länder düzeyinde ilave kanuni yetkilerin yaratılması gerekip gerekmediği incelenmelidir. Hepsinden önemlisi, yukarıda bahsedilmiş olan amaçlar, mekanizmalar ve kurumlar ilgili federal ve Länder makam ve mercileri ve iş dünyası tarafından sürekli bir uygulama süreci ile içselleştirilmelidir.

İSRAİL

Siber tehdit ve siber saldırı konusunda en iyi güvenlik ve savunma strajesine sahip ülkelerden biri de İsrail'dir. İsrail'in gelişmiş siber saldırı yetenekleri vardır ve ofansif bir strateji benimsemişlerdir. Ordu içinde "Birim 8200" adı verilen Subay, MOSSAD ajanları ve emekli askerlerden oluşan bölüm MOSSAD'ın içindeki özel birimle birlikte İsrail'in siber saldırı gücünü oluşturmaktadır.

İsrail, siber savunma ve istihbarat faaliyetini yaparken "C4ISR adlı" bir sistemler bütünü de kullanmaktadır. Tam Açılımı Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance: Komuta, Kontrol, Muhabere, Bilgisayar, İstihbarat, Gözetleme, Keşif; yani sağlıklı bir muharebe yürütülmesi için gerekli olan fonksiyonlar ve sistemlerin tümü denebilir. Bir keşif İHA'sı da C4ISR sistemidir, istihbarat uydusu da, askeri haberleşme sistemi gibi sistemler içerir.

İsrail'in siber güvenlik stratejisi içerisinde ülke içindeki bilgisayarların güvenliğini sağlamak ise iç istihbarat kurumu Şin Bet'in görevidir. Başbakan Netanyahu'nun da siber tehdidi "*Füzelerle yapılacak bir savaş kadar tehlikeli*" olarak yorumladığı ve bu düşünceyle ordu içinde özel bir birim kurduğu ifade edilmektedir.[50]

"Birim 8200" aynı zamanda yetişmiş donanımlı personel temini konusunda akademik bir rol üstlenmekte ve eğittiği personeli istihbarat ve siber güvenlik konusunda çeşitli birimlerde görevlendirmektedir.[51]

İsrail'in siber savunma ve siber güvenlik politikasına göre; ordu ve sivil otoriteler gerekli teknik alt yapısı ve tam donanımlı eğitimli personeliyle, internet üzerinden gelebilecek siber tehditlere karşı her an hazır durumdadırlar. Negev çölündeki üs bölgesinde yüksek teknoloji

[50] http://www.nogw.com/download2/-0_kibbutz-urim_secret_base.pdf
[51] http://www.military.com/features/0,15240,210486,00.html

ekipmanlar ve antenler tüm dünyadaki internet ve data trafiğini sürekli takip etmektedirler.[52]

İsrail gerek jeopolitik konumu gerekse de ulusal güvenlik politikaları gereği, siber savaş ve siber tehditler ile mücadeleyi istihbarat faaliyetleri ve askeri hareket kabiliyetiyle birleştirmiştir.

İsrail'in kritik hükümet sistemleri herhangi bir siber tehditten etkilenmemesi için intranet gibi, internetten bağımsız olarak çalışabilen ve genellikle hassas ve gizli bilgileri taşıyan ağlar üzerinde çalışır. Günümüzde birçok ülke hala gizli ve kritik ulusal sistemlerini internet tabanlı sistemlerde tutmaktadır ve sırf bu yüzden internet üzerinden gelebilecek her türlü siber saldırı tehditlerine her an açık durumdadırlar. İsrail kritik sistemlerini intranet sistemleri üzerinde tutarak nispeten dışarıdan gelen tehditlere karşı kendini kapamış durumdadır.

İnternet güvenlik şirketi McAfee'nin desteklediği bir araştırma sonucuna göre İsrail, Finlandiya ve İsveç sanal saldırılara karşı en hazırlıklı ülkelerdir.

[52] Le Monde Diplomatique, 2010 September, "Israel's Omniscient Ears: Israel's Urim Base in the Negev Desert is among the most important and powerful intelligence gathering sites in the world. Yet, until now, its eavesdropping has gone entirely unmentioned," http://mondediplo.com/2010/09/04israelbase

SİNGAPUR

Singapur Cumhuriyeti, 4,7 milyon nüfuslu bir ada devletidir. Yaklaşık %77'lik bir internet kullanım oranına sahip Singapur Cumhuriyeti, dünyanın en gelişmiş İnternet altyapılarından birine sahiptir.[53] E-devlet projelerini önemli ölçüde hayata geçirmiş olan Singapur hükümeti, kamu web sitelerine ve önemli bilgi sistemlerine (santraller, tren otomasyon sistemleri gibi) saldırılara yönelik bir erken uyarı sistemi kurulması için 2008 yılında çalışmalara başlamıştır. Asıl amaç ulusal düzeyde proaktif önlemlerin alınması sağlamaktır. Bu doğrultuda hiyerarşik olarak İçişleri Bakanlığı'na bağlı Dahili Güvenlik Departmanının bir alt-birimi olarak, 1 Ekim 2009 yılında Ulusal Siber Güvenlik Merkezi (the Singapore Infocomm Technology Security Authority – SITSA) kurulmuştur.

SITSA'nın temel görevleri;

(a) Stratejik devlet projelerinde bilişim güvenliği danışmanlığı sunmak,

(b) Singapur'un bilişim güvenliğini artırmaya etkili kuruluşlarla işbirliği kurmak,

(c) Bilişim güvenliği ve tehditleri alanlarında teknoloji geliştirme çalışmaları sürdürmek,

(d) Singapur'un maruz kalabileceği dahili veya harici bir siber saldırı durumuna karşı planlama, hazırlıklı olmayı ve karşılık verilmesini sağlamak,

(e) Altyapıdaki açıkları tespit etmek, teknik kapasiteyi geliştirmek amacıyla operasyonel planlar geliştirmektir.

Siber tehditleri önleme ve etkilerini azaltmak için bilgi paylaşımı önemlidir. Bazı kurumlar çeşitli nedenlerle siber güvenlik tehditleriyle ilgili olarak bilgi paylaşmaktan çekinebilmektedirler. Benzer şekilde kamu hizmetlerinin sunumuna katılan özel sektör oyuncuları ticari itibarın korunması veya ticari sırların ifşa edilmesi endişeyle siber güvenlik

[53] *Internet Usage in Asia, http://www.internetworldstats.com/stats3.htm (Son erişim 4 Mar 2011)*

tehditlerini veya vuku bulmuş olaylarla ilgili olarak bilgi paylaşmaya çekinebilmektedirler. Esasında SITSA kurulmuş olsa da, ilgili kamu kurum ve kuruluşlarının kendi siber güvenlik politikalarını belirleme ve uygulama hususlarında sorumlulukları devam etmektedir. SITSA yatay düzlemde tüm kamu kurum ve kuruluşlarına siber güvenlik politikalarının güçlendirilmesi hususunda yardımcı olmaktadır. Ayrıca SITSA ilgili kurumların ve paydaşların (kritik altyapıları yöneten kurum veya kuruluşların) güven içerisinde bilgi paylaşımı yapabilecekleri ve her türlü bilgiyi kendi hukuki durumlarına halel getirmeksizin doğrudan paylaşabilecekleri bir bilgi ağı kurmuştur.[54] Bu şekilde ülke genelinde koordinasyon sağlanmaktadır. Siber güvenlik tehditleriyle mücadele etmek amacıyla SITSA geniş yetkilerle donatılmıştır. Ayrıca, özel sektörün siber güvenlik alanındaki tecrübelerinden faydalanmak amacıyla her seviyede işbirliğini geliştirmede SITSA'nın yetkisi bulunmaktadır. [55]

SITSA ile ilgili olarak henüz birinci faz tamamlanmış olup güvenlik ve acil durum kritik bilişim altyapılarının takibi için gerekli olan sistem kurulmuştur. Singapur ayrıca sınıraşan siber güvenlik tehditleri ile mücadele için Interpol ile işbirliği içindedir ve SITSA bünyesinde Interpol ile ortak çalışmaların sürdürüleceği yeni bir alt birimin 2013 sonlarında hizmete girmesi planlanmaktadır.

[54] Buckland, Benjamin S.; Schreier, Fred; Winkler, Theodor H. Democratic Governance Challanges of Cyber Security. The Geneva Centre for the Democratic Control of Armed Forces (DCAF), 9-Sep-2010. http://dspace.cigilibrary.org/jspui/bitstream/123456789/29509/1/Democratic%20Governance%20Challenges%20of%20Cyber%20Security.pdf?1 (Date of access 4 March 2011)

[55] *Ministry of Home Affairs, Press Releases, http://www.mha.gov.sg/news_details.aspx?nid=MTU2MQ==-0tPkaml9VAY= (Son erişim 4 Mar 2011) Deibert, Ronald; et al. Access Denied: The Practice and Policy of Global Internet Filtering. Cambridge, Mass: MIT Press, 2008.*

NATO – Kuzey Atlantik Antlaşması Örgütü

NATO'nun Siber Savunma Politikası - *Kısa bir bakış*

Arkaplan

21. Yüzyılda güvenlik anlayışı, geleneksel tanımların oldukça dışına çıkmış durumdadır. Günümüzün modern toplumları ve ekonomileri tamamen elektronik ağlar ve kablolarla birbirine bağlanmış, iletişimlerini bilgisayar ve akıllı elektronik cihazlar üzerinden sağlar duruma gelmiştir. Kullanımı gittikçe yaygınlaşan bilişim sistemleri, kritik altyapıların ve toplumların fiziksel güvenliğini dahi etkileyecek seviyeye gelmiştir. İşte bu durum, siber güvenliğin tehdit düzeyinin ne denli önemi haiz olduğuna dair fikir vermektedir.

NATO'nun 2010 Stratejik Konsept'inde **Siber Güvenlik** konusu " *… siber saldırılara karşı yeteneğimizi geliştirerek saldırıları tespit etme, koruma ve engelleme alanlarında çalışmalar yapma..*" pasajıyla vurgulanmıştır. İşte bu arka plan hazırlıkları 2010 Lizbon Zirvesinde aksiyon planına dönüşmüş, NATO'nun ihtiyacı olan Siber Savunma Politikası dokümanı hazırlanmasına karar verilmiştir. Konsept dokümanı alınan bu kararla 2011 Mart'ında hazır edilmiş, sonrasında 8 Haziran 2011'de NATO Savunma Bakanlarının onayıyla uygun görülerek yürürlüğe girmiştir.[56]

Hedefler

- NATO'nun temel görevlerini yerine getirmesi esnasında siber güvenlik unsurlarını dikkate alması ve NATO yapıları ile iş süreçlerinde bu unsuların tam entegrasyonunun sağlanması
- NATO ve üye ülkelerin siber saldırılara karşı etkin savunma yapabilmesi
- NATO'nun kendi ağlarının merkezi kontrolü ve savunmasıyla birlikte siber savunma yetkinliklerinin geliştirilmesi
- NATO'nun bütün temel işlevlerini kapsayacak siber savunma ihtiyaçlarının tesbiti ve hayata geçirilmesi

[56] Defending the Networks- The NATO Policy on Cyber Defence, NATO Public Diplomacy Division

- Uluslararası organizasyonlar, sivil toplum kuruluşları, üye ülkeler, akademik çevreler ve özel sektör ile ortak çalışma ve fikir alışverişi yürüterek siber savunma yetkinliklerini geliştirme

NATO'nun Siber Savunma Politikası kapsamında değerlendirilen hususlar olarak öne çıkmaktadır.

Ana hatlarıyla NATO Siber Savunma Politikası

Temel Noktalar

NATO, üye ülkelerle iş birliği içinde yürüttüğü temel ve kritik işlemlerin kesintisiz gerçekleştirilmesine büyük önem vermektedir. Bu önem, **Siber Savunma Politikası'nın** da omurgasını oluşturmakta ve temel hedef olarak "NATO'nun kendi iletişim ve bilgi sistemlerinin her türlü siber saldırıya karşı korunması" ilkesi benimsenmektedir.[57] Bu temel hedef doğrultusunda varılmak istenen gayeye ulaşabilmek için her geçen gün çeşitlenen siber saldırılara karşı bilgi birikimini geliştirmek ve kendi sistemlerini bu bilgi birikimiyle destelemek, NATO'nun üzerinde önemle durduğu noktalar arasında yer almaktadır.

Hedefler

NATO, siber saldırı anında etkili cevap verme mekanizmalarını geliştirme hedefinin yanı sıra planlama ve yetkinlik boyutlarında da ciddi çalışma içindedir. Bunu sağlayabilmek için bütün üye ülkelerle birlikte organize hareket etmesi NATO'nun olmazsa olmaları arasındadır denilebilir. İşte bu noktada, NATO Defense Planning Process (**NDPP**) yapısı devreye girerek ulusal savuma mekanizmalarının NATO ile haberleşmesini sağlar. Bu yapı ile NATO üye ülkelerin ağlarıyla tam entegre biçimde büyük bir haberleşme altyapısı kullanır ve koordinasyon başarıyı getirir.

Prensipler

Siber savunma amacına hizmet eden gayretlerin temel ekseni; önlem, saldırı sonrası toparlanma ve tekrar etmeyen işlemler üzerindedir. **Saldırı önlemleri** ve **saldırı sonrası**

[57] NATO and Cyber Defence, Rex B. Hughes, Ap:2009nr1/4

tahribatın giderilmesi, saldırının yapılması ihtimalinin her zaman olması nedeniyledir. Benzer savunma mekanizmalarının tekrarlanmaması, çift kaynaktan beslenmenin oluşturabileceği sıkıntılar nedeniyle bu konuda da çalışmalar yapılmaktadır.

Tepki

Stratejik Konseptte belirtiliği gibi NATO, kendini ve üye ülkelerin sistemlerini siber tehditler dahil olmak üzere her türlü saldırıya karşı koruma hedefini benimsemiştir. NATO'nun **Siber Savunma Politika Dökümanında** belirtildiği gibi üye devletlerin saldırı kurbanı olması NATO'yu doğrudan ilgilendirir. Erken uyarı sistemleri, farkındalık oluşturma ve bilgi paylaşım ağları bu nedenle NATO'nun kurduğu ve yönettiği yapılara örnek olarak verilebilir.

Herhangi bir saldırı veya sıradışı bir siber tehdit olayı karşısında, NATO üye ülkeleri koordineli bir savunma işbirliğiyle koruma altına alır. Bu noktada **NATO Computer Incident Response Capability (NCIRC)** devreye girer ve kendi bilgi alt yapısıyla saldırıları karşılama ve cevap verme yetkinliğini kullanır.

NATO ve Siber Güvenlik Geçmişi

NATO bilgi sistemlerine karşı yapılan sayısal ataklar ilk defa 1990'ların sonunda NATO'nun Balkanlar'a yaptığı operasyonlar sırasında raporlanmıştır. Bundan sonra, birçok güvenlik olayı NATO web sitelerinin içeriğinin değiştirilmesi ve e-posta sunucularının ele geçirilmesi şeklinde gerçekleşmiştir. Ayrıca, NATO bilgi sistemleri kapsamındaki sayısal iletişimlerin kontrol altına alınması, operasyonel servislerin kesintiye uğratılması da çok ciddi kaygılar uyandırmıştır.

Bütün bu gelişmelerin sonucunda, 2002 yılındaki Prag Zirvesi'nde, NATO üyesi ülkelerin devlet başkanları, **"NATO bilgi sistemlerinin sayısal ataklara karşı savunma yeteneklerinin güçlendirilmesi"** konusundaki deklarasyona imza attılar.

2002'deki Prag zirvesinde imzalanan deklarasyon, birliğin sayısal güvenlik ile ilgili durumunu geliştirici bazı dahili NATO aktivitelerinin başlatılmasını sağlamıştır. En önemli ve kapsamlı

çalışma, NATO Bilgisayar Olaylarına Müdahale Yeteneği kurulması **(NCIRC Computer Incident Response Capability)** projesinin 2003 senesinde başlatılmasıdır. NCIRC 2006 senesinden bu yana faaliyet göstermekte; NATO bilgisayar ağlarına yönelik sayısal ataklara müdahale etmektedir.

Nisan ve Mayıs 2007'de Estonya bilgi sistemleri, daha doğrusu Estonya'ya karşı gerçekleştirilen sayısal ataklar sonucunda sayısal savunmanın tüm ülkeyi ilgilendirdiği ve ulusal bir konu olduğunun anlaşılması Siber Güvenlik anlayışının gelişmesi açısından kritik bir adımdır. Bu nedenle, konunun siyasal ve stratejik seviyede de ele alınması gerektiği anlaşılmaktadır.

2007'de Estonya bilgi sistemlerine yönelik gerçekleştirilen sayısal ataklardan sonra, NATO'ya üye ülkeler olayın değerlendirmesini yapmak üzere bir araya gelmeye ve NATO'nun sayısal savunma yeteneklerini artırmak için gerekli adımları atmaya karar vermişlerdir.

Bu kapsamda, 20 Aralık 2007'de **"NATO Sayısal Savunma Strateji Belgesi**" yayınlandı. 17 Nisan 2008'de ise "NATO Sayısal Savunma Yönetim Otoritesi" – CDMA kuruldu. 2009 senesi başında, CDMA için operasyon konsepti (Concept of Operations-*CONOPS)* geliştirildi ve kabul edildi.

NATO'nun kurduğu yapılar bununla sınırlı kalmamış, teknolojik yetkinliğini geliştirmesi için yaptığı yatırımlar devam etmiştir. **Cooperative Cyber Defence (CCD)** ve **Centre of Excellence (COE)** bu kapsamda kurulan merkezlere örnek olarak verilebilir. Estonya'ya yönelik gerçekleştirilen saldırılar, bu merkezin de Tallinn'de kurulmasına zemin hazırlamıştır. Üye ülkelerden çalışanların da aktif rol aldığı CCD-COE merkezinde, NATO'nun uzun dönemde siber yetkinliklerini nasıl geliştirebileceği üzerine araştırmalar yapılmaktadır.

NATO'da yeni yaklaşım doğrudan teknik ve operasyonel desteğin sağlanmasını da içeren bir yapıya sahiptir. NATO sayısal savunma hızlı reaksiyon takımının, siber ataklara maruz kalan üye ülkeye, ülkenin de talep etmesi durumunda gönderilmesi buna bir örnek olarak verilebilir.

NATO'nun sayısal savunma yeteneğinin asıl sorumluluğu, görevleri desteklemek için NATO tarafından işletilen bilgisayar ağlarını korumaktır. NATO şu anki yapısıyla, herhangi bir üye ülke eğer sayısal atak altında ise ülkeyi korumakla ve ülkeye yardım teklif etmekle yükümlüdür.

Burada önemli bir noktanın altını çizmekte fayda var. NATO üyesi iki ülke, ABD ve İngiltere, sayısal saldırı yeteneklerini geliştirmekteler ve bunu ülkenin ulusal istihbarat kuruluşu ile koordineli (hatta aynı kurumların içinden) yönetmektedirler.[58]

Ancak NATO ise, sadece sayısal "savunma" yeteneği kurmuştur ve bunu geliştirmektedir. Bu durum NATO organizasyon yapısının hedefleriyle, ülkelerin münferit olarak kendi çıkarlarını koruma ve siber teknolojileri gerektiği zaman menfaatlerine yönelik saldırı amacıyla bile kullanma hedefinin farkını gözler önüne sermektedir.

Sonuç olarak NATO, son yıllarda etkisi ülkeleri aşarak küresel bir tehdit haline dönüşebilecek siber saldırılara karşı farkındalığı yüksek bir organizasyondur. Bu alanda gerek teknik gerekse yönetsel açıdan her türlü yatırımı yapan NATO, üye ülkeleri de bilinçlendirme ve yeri geldiğinde teknik destek de dahil olmak üzere her türlü yardımı yapan etkin bir kuruluş olarak öne çıkmaktadır. Bu açılardan kurduğu yapı ve **CCD-COE, CDMA** gibi savunma mekanizmaları, üye ülkelerin referans olarak kullanabileceği seviyede başarılı merkezler olarak, hem NATO üyesi ülkelere hem de küresel anlamda bütün toplumlara örnek olarak siber güvenlik farkındalığı oluşturmada etkin rol oynamaktadır.

[58] ANIL, Süleyman, Cyber Security in NATO and Nations, Cyber Warfare Symposium, 10 December 2009, Ankara

ITU (Uluslar arası Telekomünikasyon Birliği)

Gelişim Tarihçesi:

2003-2005 : WSIS(World Summit of the Information Society) ICT kullanımlarına güven duyulması konusunda aksiyonların tek sorumlusunu ITU olarak görevlendirdi.

2007: ITU Genel Sekreterliği, siber güvenlik konusunda uluslararası bir kapsam yaratmayı hedefleyen GCA (Global Cybersecurtiy Agenda) dokümanlarını yayınladı.

2008 – 2010: ITU üyeleri GCA dokümanını uluslararası birlikteliği sağlayacak içerik olarak kabul ettiler ve onayladılar.

Teknolojinin gelişmesiyle internetin modern toplumların vazgeçilmezi haline gelmesi, bireylerin günlük hayatlarını yürütebilmeleri için pek çok konuda internet üzerinden online işlemler yapıyor olması ve iletişimde sınırların internet aracılığıyla kaldırılması siber saldırıların ülkeler ve ekonomiler için daha büyük tehditler haline gelmesine yol açmıştır. Bu bağlamda her geçen gün siber güvenlik tehditleri de farklılaşmakta ve kendini geliştirmektedir. Çeşitlilik düşünüldüğünde siber güvenlik tehditlerine karşı verilecek mücadelede uluslararası bir platform yaratma ihtiyacı doğmuş ve global standartların oluşturulması için ITU görevlendirilmiştir.

Birçok ülkede, özellikle de gelişmekte olan ülkelerde, halen bilişim acil durumlarına karşı pek az tedbir alınmaktadır. Bilişim ağlarının kendi içlerinde ara bağlantılar ile birleştirilmiş olması sebebiyle, siber güvenlik konusunda daha az tedbir almış olan ülkelerin ağlarına yapılacak saldırılar, bu ara bağlantılar üzerinden diğer ülkeleri de etkileyebilir. Dolayısıyla, üye ülkelerin ulusal siber güvenlik acil müdahale merkezleri kurmaları şiddetle tavsiye edilmektedir

İnternetin karmaşık ve yaygın ağ yapısı, içerik kontrolünü ve siber saldırıların kaynaklarını tespit etme konusunu oldukça zor bir hale getirmektedir. Bunların dışında bilgi teknolojilerinin değişken yapısı kanuni boşluklardan yararlanabilecek açıklar yaratmakta ve bu durum siber tehditlere karşı mücadeleyi daha da zorlaştırmaktadır. Bu sebeple ITU, siber güvenliğin tüm ülkelerin önemli bir gündemi olduğunu varsayarak toplu hareket etmeyi sağlayacak global bir mesele olan siber tehditlere global çözümler üretme sürecini

başlatmıştır. Kritik hedefler; tüm ülkelerin siber güvenlik, izinsiz girişlere karşı koruma programları ve kritik kaynaklarda manipülasyonlar konularında aynı bilgi seviyesine erişmelerini sağlamaktır. Belirlenecek stratejilerin tüm ülkelerde efektif bir şekilde hayata geçebilmesi için bütün bölgesel ve ulusal dinamikleri kapsar nitelikte olması gerekmektedir.

ITU 3 ana sektörden oluşur: **Radyo İletişim Sektörü (ITU-R), Standartlar Sektörü (ITU-T), Telekomünikasyon Geliştirme Sektörü (ITU-D)**

Bu bağlamda 2003-2005 WSIS toplantısına katılan tüm liderler ITU' yu siber güvenlik konularında tüm koordinasyonu sağlama ve güven duyulan ICT platformları oluşturma görevlerinde tek sorumlu ilan etmişlerdir. Buna bağlı olarak yapılan çalışmalar ile 17 Mayıs 2007 yılında siber güvenlik için global bir çerçeve oluşturacak GCA (Global Cybersecurity Agenda) yayınlanmıştır.

GCA temel olarak aşağıdaki başlıklarda incelenebilir;

- Hukuki Tedbirler
- Teknik ve Prosedürel Tedbirler
- Siber güvenlik araçları
- Ulusal bir siber güvenlik programında bulunması gerekenler

HUKUKİ TEDBİRLER

Yasal süreçlerdeki boşluklar, ülkeler arası hukuki farklılıklar, siber güvenlik tehditlerini ve suçlularını takip etme ve inceleme süreçlerini zorlaştıran adımlardır. İnternetin global yapısı onu tehdit eden unsurlara da global çözümler üretmeyi gerektirmektedir. ITU siber güvenlik konusunun hukuksal çerçevesini iki ana dokümana bağlı kalarak çizmektedir. Bunlardan biri Siber Güvenlik Mevzuatı için hazırlanmış '*ITU Uygulamaları'* dokümanı ve '*Siber Güvenliği Anlamak: Gelişen Ülkeler için Kılavuz'* ismiyle yayınlanmış dokümandır.

Siber Güvenliği Anlamak: Gelişen Ülkeler için Kılavuz: Dokümanın temel hedefi bütün ülkelerde büyüyen siber tehditlerin sonuçlarıyla ilgili yeterli algıyı yaratmaktır. İçeriğinde siber suçların hukuki boyutlarıyla ilgili kapsamlı bir anlatım yer almaktadır. Bununla beraber

genel yaklaşım gelişmekte olan ülkelere yöneliktir. Kılavuzda 6 ana bölüm bulunur. Bunlar; Giriş bölümü, siber suçlar hakkında genel açıklamalar, soruşturma ve cezai takibat aşamasındaki zorluklar, bazı ulusal veya uluslararası kurumların siber tehditlere karşı aldığı aksiyonlar, farklı hukuksal yaklaşımlara ait örneklemeli analizlerdir.[59]

Siber Güvenlik Mevzuatı için hazırlanmış ITU Uygulamaları Dokümanı: Bu doküman ITU üyesi ülkelere uyumlu hale getirilmiş bir siber suçlar kanunu yaratma sürecinde ortak hukuki dili ve referansları sağlayacak materyalleri sağlamayı hedefler. Böylelikle her ülkeye siber suçlar yasalarını taslak haline getirme ve yürürlüğe koyma sürecinde kaynak alabilecekleri kılavuz sağlanmış olur.[60]

Bu uygulamaların 3 temel bölümü mevcuttur.

1. Örnek bir dil kullanımını açıklayan belirli örnekler
2. Farklı ülkeleri hukuksal anlamda kıyaslayan bir uluslararası siber suçlar matrisi
3. Referans olabilecek pek çok değerli kitap, makale, çalışma dokümanları, siber suç kanunları vb.

TEKNİK VE PROSEDÜREL TEDBİRLER

Bilişim teknolojileri günümüz bilgi toplumlarında hayati bir önem taşımakla beraber, hızla değişen ve gelişen altyapısı sebebiyle her geçen gün bu alana yönelik kötüye kullanımlar artmakta ve organize suç niteliğine kavuşmaktadır. Bu tip kötüye kullanımlara örnek olarak, izinsiz girişler ve modifikasyonlar yaratacak kötücül yazılımlar ile bilgi teknolojilerinin bütünlüğünü ve güvenilirliğini sarsmak verilebilir.

ITU Standart Çalışmaları: IT standart belirleme çalışmaları özel sektörü ve devlet kurumlarını bir araya getirmesi ve güvenlik politikaları ile güvenlik standartlarının uyumluluğunu sağlaması anlamında tekil bir göreve sahiptir. Standartların netleştirilmesi güvenlik konusundaki kırılımların doğru adreslenmesi adına çok önemli protokollerdir. Özellikle IP tabanlı sistemler, NGN sistemlerinde seriş kalitesi, şebeke yönetimi, mobilite, faturalandırma

[59] ITU Global Cybersecurity Agenda // ITU Küresel Siber Güvenlik Gündemi
http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf
[60] ITU Ulusal Siber Güvenlik Strateji Kılavuzu
http://www.itu.int/ITU-/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

süreçleri hakkında uluslararası platformlar tasarlanması hedeflenir. Bu hedef doğrultusunda ITU tarafından belli başlıklarda farklı tavsiye kararları yayınlanmıştır. Bu kararların içerikleri aşağıdaki gibidir;

H.235.x Tavsiye Kararları: IP tabanlı multimedya uygulamalarına ait altyapıları düzenleyen ve gizlilik hizmetleri sağlayan kararlardır. Multimedya uygulamaları üzerinden iletişim kuran kullanıcıların onay ve yetki süreçlerinde verilerinin siber tehditlere karşı korunması sağlanmaktadır. Gerçek zamanlı şifreleme metotları ile güvenlik katmanları oluşturulmaktadır.

J.170Tavsiye Kararları: IPCablecom mimarisi için güvenlik düzenlemelerini içerir ve televizyon operatörlerine güvenli IP hizmetleri sağlama konusunda yönlendirir.

X.805 Tavsiye Kararları: Bu kararlar tüm iletişim şebekeleri için baştan sona güvenlik sağlamayı hedeflemektedir. Bu adımda şebeke saldırılarına karşı tedbirleri, hırsızlık ve fraud, gizli dinlemeler, yetkilendirme için telebiometri, telekomünikasyon süreçlerinde güvenlik gibi pek çok farklı konuyu içermektedir.

X.509 Tavsiye Kararları: ITU tarafından geliştirilen en önemli standartlar olarak bilinen ve günümüzde kullanımı olan tüm şebekede elektronik yetkilendirme standartlarıdır. Tüm dijital sertifika sistemlerinin temeli olan Açık Anahtar Altyapısının (PKI) referansları bu standart sayesinde belirlenir. Web arayüzleri ve sunucular arasındaki entegrasyonlarda transfer edilen datanın güvenliğini sağlayan şifreleme anahtarlarının güvenilir yapısını sağlamaktadır. Ek olarak maillerin onaylanması ve güvenliğini sağlayan dijital sertifikayı destekler.

ITU-T X.1205 Tavsiye Kararları: En son onaylanan "Siber Güvenlik Genel Açıklamaları" olarak bilinen kararlardır. Siber güvenlik konularına ve siber tehditlerin sınıflandırmalarına ait tanımları içerir. Siber güvenlik ortamının normlarını ve risklerini tartışır, olası stratejileri belirler, güvenli iletişim tekniklerini inceler.

Halen ITU Çalışma Grupları farklı konularda ve aktivitelerde incelemelerine devam etmektedir. Bunlardan Telekom Standartları sektörünün oluşturduğu Çalışma Grubu 17 tüm çalışmalarda lider konumundadır.

2002 yılında ITU tüm standartları ve organizasyonları takip etmeyi ve bu gruplarla ortak çalışmalar yapmayı hedef olarak belirledi. Çalışma Grubu 17 bu süreçlerde lider rolündeydi ve yüzün üzerinde iletişim güvenliği konularında hazırlanan ve temel olarak X serisi olarak bilinen tavsiye kararını onayladı. Bu süreçte kararlar bazen salt kendi bünyesinden bazen de ISO/IEC veya diğer organizasyonlarla ortaklaşa çıkartılmıştır. Düzenli olarak, ITU-T Çalışma gruplarının düzenlediği ITU-T Tavsiye Kararlarının hayata geçirilmesi anlamına gelen "Telekomünikasyon ve Bilişim Teknolojilerinde Güvenlik" kitapçığını yayınlanmıştır. (4. Versiyon 2009 yılında)

Çalışma Grubu 17'nin rolü WTSA (World Telecommunication Standardization Assemblies) 2008'de Johannesburg'da alınan pek çok uzlaştırma (50-52-58) kararıyla onaylanmıştır.

Yol Haritası: Bilgi Teknolojileri Standartları Yol Haritası ENISA (European Network and Information Security Agency) ve NISSG (European Network and Information Security Agency) katılımlarıyla ITU Çalışma Grubu 17 tarafından Ocak 2007'de yayınlanmıştır. Yol haritasının 5 ana bölümü bulunmaktadır.

BÖLÜM 1: ITU, ISO, IEC, IETF, OAIS, ATIS, ETSI, IEEE, 3GPP ve 3GPP2 gibi farklı standart organizasyonlarının yapıları ve işleyişleri ele alınır.

BÖLÜM 2: Onaylanmış bir güvenlik standartları veri tabanı sağlanır.

BÖLÜM 3: Geliştirilmekte olan standartları ve standart belirleyen kurumlar arasındaki ilişkileri içerir.

BÖLÜM 4: Gelecek ihtiyaçları ve taslak standart önerilerini kapsar.

BÖLÜM 5: Uygulama örneklerini içerir.

ITU RADYOTELEKOMÜNİKASYON: ITU Radyo telekomünikasyon sektörünün görevi rasyonel, eşit dağılımlı, etken ve ekonomik radyo frekansı kullanımı için doğru platformu yaratmaktır. Bu sektörün regülasyonları 9 kHz'den 400 GHz'e kadar olan aralıktaki frekanslara yöneliktir ve nasıl paylaşım yapılacağı konularını kapsar. WRC (World Radiocommunication Conferences) 3-4 yıllık periyotlarda uluslararası anlaşmalarla radyo frekans spektrum

süreçlerini düzenler. Bu düzenlemelerle ilgili pek çok uzlaşma kararı yayınlanmıştır ve ITU 3G şebekesinin güncel şebekelerle kıyaslanabilir olması gerektiğini savunmaktadır. Ek olarak ITU dijital uydu sistemleri için şebeke yönetim mimarisinde güvenlik sorunlarına ve uydu sistemlerinde transmisyon kontrol protokollerinin performans artışı gerekliliğine dikkat çeker.

ITU global işbirliğini sağlamak adına uzmanları arasında iletişimi ESCAPE (Electronically Secure Collaboration Application Platform for Experts) adı verilen bir platform üzerinden sağlamaktadır. Bu ortam farklı ülkelerin siber uzmanlarının yetkileri dahilinde kaynak havuzlarından yararlanabildikleri, uzaktan erişim ile iletişime geçebildikleri bir uygulamadır. Bu yapıda bir iletişim özellikle kriz durumlarında oldukça fayda sağlamaktadır.

ITU'NUN SİBER GÜVENLİK ARAÇLARI

IMPACT Security Assurance Division

IMPACT, BİT uzmanları ile işbirliği yaparak, küresel "Best Practice" kılavuzları hazırlamaktadır. Aynı zamanda, talep edilmesi halinde, devlet kurumları veya kritik önem taşıyan altyapı şirketlerinin sistemleri üzerinde bağımsız güvenlik denetimleri gerçekleştirmektedir. Ek olarak, siber güvenlik için bağımsız, uluslararası olarak tanınan bir sertifikasyon kurumu olarak da görev yapmaktadır.

ITU National Cybersecurity/CIIP SelfAssessment Tool

ITU Ulusal Siber Güvenlik/ CIIP Öz Değerlendirme Aracı, ITU üye devletlerinin siber güvenlik ve CIIP (Critical Information Infrastructure Protection – Kritik Bilgi Altyapısı Koruması) konusundaki politikalarını belirlemeye yardımcı olmayı amaçlayan bir araçtır.

ITU Toolkit for Promoting a Culture of Cybersecurity

Bu araç, gelişmekte olan ülkelerde, siber güvenlik konusunda KOBİ'lerin, tüketicilerin ve son kullanıcıların bilinçlendirilmesi için atılabilecek adımları gösterecek bir kılavuz oluşturmaktadır.

ITU Botnet Mitigation Toolkit

Gelişmekte olan ülkelerin büyüyen botnet (zombi bilgisayar ordusu) sorunu ile başa çıkabilmelerini sağlayacak bir araçtır. Botnetlerin bulunması ve etkilerinin sonlandırılmasına hizmet eder.

AVRUPA BİRLİĞİ (AB)

Siber Güvenlik konusunda AB'de temel adımlar

- 1 Eylül 2005: Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tam anlamıyla faaliyete başladı.
- Mayıs 2007: Çevirim içi terörizmi gözlemlemek için Avrupa Polis Ofisi (Europol) tarafından 'Webi (ağı) Kontrol Et" isimli güvenlik portalı kuruldu.
- Nisan 2010: AB bakanları, merkezi siber suç ajansına ihtiyacın araştırılması için Komisyon'a çağrıda bulundu.
- Ekim 2010: Komisyon bilgi sistemi saldırılarına karşı yeni bir önerge sunmayı planlıyor.
- 9 Aralık 2010: Çevrimiçi radikalleşmeyi de kapsayan Terörle Mücadele Çerçeve Belgesi'nin tüm üye ülkelerde uygulanması için son gün.

Konular

2020 itibariyle internet güvenliği öncelikli konulardan birini teşkil ediyor.

AB'nin internet güvenliği ajansı ENISA, bilgi ağlarını güvenlik altına almaya çalışmakta, fakat şu anki durumda ajans başa çıkmasını sağlayacak yasal dayanağı olmayan bir merkez konumundadır.

Örneğin 2008'de ajans mobil iletişimin güvenlik tehditlerine karşı ne kadar savunmasız olduğu konusunda bir bildiri yayınlamıştır.

Siber suçlarla mücadelede Europol de aktif çalışmalar içindedir. Kurum, çocuk pornografisi gibi sınır ötesi siber suçların engellenmesinde yürütme organlarına yardım adına faaliyet gösteren çeşitli çalışma gruplarını denetlemektedir.

Buna karşın, gittikçe artan bir kullanıcı sayısının sosyal paylaşım sitelerinde bilgilerini paylaşmaları, siber suçun çoğalmasına zemin hazırlamaktadır.

Siber suç

Sosyal medya sitelerinden yayılan riskler web güvenlik şirketi olan Sophos'un en son yayınlanan raporundaki elektronik tehlike listesinin başında gelmektedir. Dijital tüketicileri rahatsız edenler listesinde ikinci sırada ise e-postalarla BlackBerry ve iPhone gibi yeni cihazlara yapılan saldırılar ve e-dolandırıcılık geliyor.

Bazı ülkelerin interneti kontrol altına almak için köklü birimleri mevcuttur. Hollanda'da Felemenk polisi siber suçla savaş için bir İnternet Ekibi kurarken İngiltere'de İnternet İzleme Derneği, yasa dışı içeriği raporlaması adına, halkın ve Bilgi Teknolojileri (BT) personelinin kullanımı için bir 'internet yardım hattı' çalışmasını sürdürmektedir.

Buna ek olarak ENISA'nın izlediği internet güvenliği konuları şu şekilde: spam, botnet, e-dolandırıcılık, kimlik hırsızlığı, menkul kıymetler borsasında hackerlar, yazılım konusundaki hassasiyetler ve kimi cihazlardaki güvenlik eksikliğidir. Kasım 2010'da ENISA tarafından siber güvenlik alıştırması yapılmış ve 27 üye yanında İsviçre, Norveç ve İzlanda ülkelerinin katılımı sağlanmıştır Bu alıştırmadan çıkan en ciddi sonuç hukuksal olarak bir işbirliğine ihtiyaç olduğudur.

Ellerinde yeterli yasal güç olmadığını fark eden AB bakanları Nisan 2010'da Avrupa Komisyonu'na çevrim içi sahtecilik ve çocuk pornografisini engellemek için merkezi bir siber suçla savaş birimi kurma konusunda talepte bulunmuştur.

AB idaresinin bildirdiği üzere siber suçun AB'ye maliyeti yıllık 750 milyar Euro ile uyuşturucu trafiğinin maliyetini de aşarak küresel GSMH'nin % 1'i olarak kayda geçmiştir.

Komisyon aynı zamanda Avrupa'da siber atağa karşı bir anında müdahale sistemi kurma çabasındadır. Buna ek olarak komisyonun hedefleri arasında bilgisayarlar için bir acil yanıt takımı (Certs) kurma planı ve ENISA'nın rolünü arttırmak da vardır.

İnternet Korsanlığı

Paris'te bulunan TERA Danışmanlık Şirketi'nin yaptığı bir internet korsanlığı araştırmasına göre, yasa dışı yüklemeler sonucu önümüzdeki 5 yıl içinde AB'de bir milyondan fazla iş ve iş çevrelerinde 240 milyar Euroluk para kaybı söz konusudur.

2009 yılı içinde hava ya da karadan yapılan yasa dışı nakliyatların üçte birini durdurmayı başaran AB gümrük yetkilileri, internet üzerinden yapılan yasa dışı mal satışında artış olduğuna dikkat çekmiştir. Verilerin olduğu yıllık yasa dışı ticaret akışı raporunu Avrupa Komisyonu'nun vergilendirme ve gümrük birliği departmanı yayınlamıştır.

Avrupa Parlamentosu çevrim içi korsanlığı ile başa çıkmak için boğuşurken pek çok AP üyesi korsanlığı suç kapsamına sokmanın fazla sert olduğu konusunda ısrar ederek bunun ticari kazanç için içeriği topluca yağmalayanlardan ziyade ara sıra dosya paylaşan insanları cezalandırmak olacağını belirtmektedirler.

Bu konuda yasa önerisinde bulunan ilk ülke olan Fransa'nın hukuku pek çok siyasetçi tarafından fazla bağlayıcı kabul edilmektedir. Yasa dışı içerik yükleyen kullanıcıların üçüncü kez de yakalanması halinde şebeke bağlantılarının kesilmesini ön gören 3 hak yasası, halen Fransız ulusal meclisinden geçmeyi beklemektedir.

Eircom internet servis sağlayıcısının yasa dışı içerik yüklendiği iddiasıyla İrlanda Plak Derneği tarafından mahkemeye verilmesinin ardından Mayıs ayında İrlanda 3 hak politikasını uygulamaya sokan ilk ülke olmuştur.

İngiliz hükümeti ve internet servis sağlayıcıları (ISPler) BT ve Talk Talk'ın arası ülkenin dijital ekonomik faturası nedeniyle açılmış haldedir. Açılan davada yüksek mahkemenin istediği yasa dışı içerik yükleyen müşterilere bir mektup yollanması, hatta bağlantılarının kesilmesidir.

Yasa dışı yükleme yapılmasında internet servis sağlayıcılarının rolü hem AB'de hem de dünya çapında tartışılan bir konudur. Mevcut durumda Avrupa Parlamentosu Sahteciliğe Karşı

Ticaret Anlaşması'nın (ACTA) yaptırımları üstüne kafa yormaktadır. Sızan bilgilere göre küresel müzakereler sonucu ISPler yasa dışı içerik yükleyen müşterilerini cezalandıracaktır.

ACTA görüşmelerine katılan 12 ülke var ve AB'nin çıkarları Avrupa Komisyonu'ndan müzakereciler tarafından temsil edilmektedir. İsveçli Yeşiller/ Avrupa Özgür Birliği üyesi ve İsveç Korsan Partisi'nin kurucu üyesi Christian Engström, ACTA'dan aldığı bilgileri kendi meclisinin üyeleriyle paylaşmasına izin verilmemesi üzerine kısa bir süre önce Avrupa Komisyonu ile görüşmeleri terk etmiştir.

Terör

Avrupa Birliği 2007 yılında 27 üye ülkenin İslam propagandası yapan verileri Lahey'deki Avrupa Polis Ofisi'nde bir havuzda topladığı "İnterneti Kontrol Et" isimli bir yüksek güvenlik portalı kurmuştur.

Yakın zaman içinde, terörle mücadelede internet servis sağlayıcıları ve internet üzerinden çalışan özel şirketlerin de işbirliğine katılmalarında artış beklenmektedir. İnternet bazlı propaganda ve radikalleşme aktivitelerine karşı sert tutum, Kasım 2008'de kabul edilen AB terörle mücadele Çerçeve Kararı'ndan doğmaktadır.

Belgede açıkça belirtildiği üzere *"internet, Avrupa çapındaki yerel terörist ağlarına ve bireylere ilham vermek ve onları mobilize etmek için kullanılıyor, ayrıca terörist yöntemler konusunda bir bilgi kaynağı olarak sanal bir eğitim kampı görevi görüyor."*

Avrupa Komisyonu, iletişim hattındaki yeni önlemler sayesinde suç işleyenlerin ve saldırı planlayanların daha kolay takip edileceğini düşünmektedir. Buna karşın, internetten bomba yapım tarifleri almak gibi dolaylı yoldan terörizmi destekleyen bireyler de bundan etkilenecektir. İnternet üzerinden olanlar da dahil radikalleşmeyi hedef alan yeni önlemler paketi 2011'de öneri olarak sunulacaktır.

Çocuk pornografisi

Buna ek olarak Avrupa Komisyonu, üye ülkelerin çocuk pornografisi yayınlayan sitelere filtre uygulamasını ve insan kaçakçılığı konusunda daha sert cezalar uygulanmasını istemektedir.

Buna karşın Avrupa Parlamentosu'nun yeni AB kanunlarının yeterince sert olacağı konusunda şüpheleri vardır.

Mart 2010'da önerilen yeni kurallarla internette çocuk pornografisi yayınlayan sitelere yasak getirilmekte, çevirim içi sohbet odalarında tacize maruz kalan kurbanların dava açma hakları doğmakta ve tacizcilerin başka bir AB ülkesinde yeniden aynı suçu işlememesi için önlem alınmaktadır.

Lakin AB öneri konusunda üye devletlerden gelen bir ihtilafla karşı karşıyadır. Pek çok üye devlete göre internetin filtrelenmesi, hükümetlerin istemediği içeriğe yasak getirmesiyle konuşma özgürlüğüne zarar verecektir. Öneriyi reddedeceğini belirten Almanya çocuk pornografisini toptan yasaklamanın içeriği filtrelemekten daha mantıklı olduğu görüşündedir.

DÜNYADAKİ BAŞARILI ÖRNEKLER ÇERÇEVESİNDE TÜRKİYE CUMHURİYETİ İÇİN ÖNERİLER

HİNDİSTAN

- Hindistan'da Bilgi Teknoloji Departmanı tarafından kurulan Acil Bilgisayar Müdahale Ekibi (CERT-In) benzeri bir yapı kurulmasının Türkiye açısından faydalı olacağı kanaatindeyiz. Hindistan'da çok başarılı şekilde işleyen bu yapı eliyle, kritik bilgi altyapısını doğrudan veya dolaylı olarak etkileyen bütün bilgisayar ve ağ sistemlerinin korunması, siber savunmayla ilgili gerekli acil müdahalelerin yapılması, devlet düzeyinde ve kritik sektörlerde güvenlik standartlarının yükseltilerek buna uyum sağlanması ve güvence altına alınması, erken uyarı sistemlerinin faaliyete geçirilmesi ve devletin organları içindeki siber güvenlik ile ilgili çalışan birimlerin koordine edilmesi sağlanabilecektir. Ayrıca siber güvenliğe ilişkin çeşitli kılavuzlar ve eylem planları, bu yapı içerisindeki uzmanlar tarafından hazırlanarak ilgili yerlere sunulabilecektir.
- Hindistan'ın siber güvenliğe ilişkin kamu-özel işbirliğini yüksek düzeyde sağlayan bir başka yapısı olan Ulusal Güvenlik Veri Tabanı (NSD) benzeri bir oluşuma gidilmesi, Türkiye sınırları içerisinde ve yurtdışında yaşayan siber güvenlik konusunda uzman kişilerin envanterinin çıkarılması, tek çatı altında toplanarak siber güvenlik konusunda hepsinin yeteneklerinden yararlanılması çok önemlidir.

AMERİKA BİRLEŞİK DEVLETLERİ

ABD'ye bakıldığında, siber uzayda söz sahibi olabilmek ve güvenli ve geliştirilebilir bir sistem oluşturabilmek için konuya birçok farklı açıdan yaklaşılması gerektiği görülmektedir. ABD'ye bakıldığında çalışmaların 6 başlık altında toplandığını görmekteyiz. Bunlar; hukuki ve regulasyonel çerçeve, ekonomik ve sosyal gelişim, ticarette gelişim, inovasyon ve girişimcilik ortamının geliştirilmesi, teknoloji altyapısı ve endüstriyel uygulamalardır.

Hukuki ve Regulasyonel Çerçeve:

ABD'ye bakıldığında siber güvenlik anlamında yönetilebilir altyapının oluşturulabilmesi için hukuki ve regulasyonel açıdan birçok çalışma gerçekleştirilmiştir.

- Siber ve ICT Altyapı Gelişimi için Devlet Desteği:
    - Ulusal Siber ve ICT (E-donuşum planı, manifestosu, vb.): Ülke durumun önemini belirtmek ve farkındalık yaratmak için belirli periyotlarda ulusal siber güvenlik raporları yayınlamış ve konuyla ilgili yaşanan gelişmeleri halk ile paylaşmıştır.
    - Kamu ve Özel Sektör İşbirlikleri ve Ortaklıklar: Siber güvenliği sağlayabilmek için ülkenin kamu ve özel sektörlerinin bir arada çalışması ve işbirliği yapması çok önemlidir çünkü yapılan saldırılar sadece kamu veya özel sektör hedefli yapılmamakta, saldırılar her iki sektörü de aynı boyutta tehdit etmektedir.
- Siber Koruma Politikası:
    - Siber Yaptırım Mekanizması ve Otoritesi: Ülke içinde bir siber yönetim mekanizmasının kurulması en önemli kriterlerden bir tanesidir.
    - Siber Güvenlik Kanunları, Yönergeleri: Siber dünyada yaşanan suç faaliyetlerini önleyebilmek adına kanun veya yönergelerin ortaya çıkarılması ortaya çıkan tehditlerin azalmasına katkıda bulunacaktır.
    - Siber Suç Tepki Mekanizmaları: Yaşanan atakları savuşturabilmek veya başa çıkabilmek için bir mekanizma veya sistemin oluşturulması gerekmektedir.
    - Uluslararası Örgütler ile İşbirliği Kapsamında Siber Güvenlik Taahhütleri: Siber tehditler tek bir noktadan gelişmediği ve birçok ülkeden aynı anda saldırı yapılabileceği için ülkeler arasında işbirliği halinde önlemlerin alınması ve gerekli yaptırımların ve mekanizmaların oluşturulması çok önemlidir.
    - Siber Güvenlik Planı (hareket planı, tepki planı, vb.): Yapılan saldırıları önlemek adına belirli bir stratejinin veya aksiyon planının ortaya çıkarılması

gerekmektedir. Saldırı anında birimlerin nasıl çalışacağı, hangi adımların atılacağı gibi operasyonel bir aksiyon planının çıkarılması büyük önem taşımaktadır.

- Siber Sansür, Spam Mekanizması, Filtreleme: Güvenlik açıklarını önleyebilmek ve belirli yaş ve bilgideki insanların kullanılarak siber atakların bir parçası olmasını önleyebilmek adına ülke dahilinde esnek ve sınırlayıcı olmayan bir spam ve/veya filtreleme mekanizmasının kurulması oluşabilecek atakların sayısının azalmasına büyük katkıda bulunacaktır.

- Politik Verimlilik, Devlet Desteği ve Kararların Hızlı Alınıp Adımların Hızlı Atılması: Ülke açısından genel bir siber politikası ve stratejisi oluşturularak devlet tarafından özel destek verilmesi ve gerekli güvenliğin sağlanabilmesi için kararların hızlı bir şekilde alınıp yine hızlı bir şekilde yürürlüğe girebileceği bir ortamın sağlanması ülkelerin siber güvenlik anlamında güçlü olmalarını sağlayabilecek önemli bir kriterdir.

- Fikri Mülkiyet Koruma, Veri Koruma Politikası: Gelişen dünyada fikirlerin ve kişisel bilgilerin önemi giderek artmaktadır ve bu yüzden ulusal bir fikri mülkiyet ve veri koruma kanunun yürürlüğe girmesi ve devam ettirilebilir bir mekanizmanın kurulması bireylerin ve şirketlerin korunması açısından büyük önem taşımaktadır.

<u>Ekonomik ve Sosyal Gelişim:</u>

- Eğitim Seviyesinin Geliştirilmesi
    - Lise mezunları oranının toplam mezun olan öğrenci sayısına oranının artırılması
    - Zorunlu öğretim ve eğitim suresi
    - Eğitim kapsamı içinde siber güvenlik ve bilişim teknolojileri farkındalığının oluşturulması ve genişletilmesi
- Teknik Becerilerin Geliştirilmesi

- İş üretkenliğinin artırılması,
- Siber güvenlik hakkında uzmanlar yetiştirecek enstitülerin kurulması
- Ar-ge alanında çalışan araştırmacı ve eğitimci sayısının artırılması
- Bilim ve mühendislik derecelerinin artırılması, spesifikleştirilmesi ve gelişen dünyaya karşılık yeni uzmanlık alanlarının oluşturulması
- Yabancı dil eğitimin yaygınlaştırılması, teknik dil becerisinin ve eğitimlerinin artırılması

Ticarette Gelişim:

- ICT ihracatının toplam ihracat içerisindeki oranının artırılması, sektörde yeni şirketlerin kurulması için teşviklerde bulunulması
- ICT ithalatının toplam ithalat içerisindeki oranının arttırılması, yeni teknolojilerin hızlı bir şekilde pazara sunulması, hızlı bilgi ve tecrübe edinilmesi
- Ticarete açıklığın arttırılması, ICT anlamında yabancı yatırımcıların ülkeye çekilmesi için gerekli teşvik ve olanakların oluşturulması, var olan iş gücünün bu sayede daha verimli hale getirilerek ülke ekonomisine katkıda bulunulması

Inovasyon ve Girişimcilik Ortamının Geliştirilmesi:

- Ar-ge'nin gayri safi milli hasıla içerisindeki oranın artırılması
- Yerli patent girişimlerinin artırılması
- Yeni ürün geliştirme ve patentleme anlamında farkındalığın oluşturulması
- Özel sermaye ve yatırım sermayesine sahip firmaların sayısının artırılması ve gayri safi milli hasılaya katkısının artırılması

Teknoloji Altyapısı:

- ICT teknolojisine erişim
    - Internet penetrasyon seviyesinin ve kullanımının artırılması
    - Mobil penetrasyon seviyesinin ve kullanımının artırılması
    - Wi-fi hotspot'larının genişletilerek internete erişimin artırılması
    - Sosyal medya kullanımının artırılması
- ICT altyapı kalitesinin artırılması
    - Sabit geniş bant penetrasyonu oranının ve kullanıcı sayısının artırılması
    - Uluslararası internet bant genişliğinin artırılması
- ICT harcamasının Gayri Safi Milli Hasıla'ya oranının artırılması
- ICT teknolojisi satın alinabilirliğinin artırılması
    - Mobil tarifelerinin daha cazip hale getirilmesi
    - Geniş bant tarifelerinin daha cazip hale getirilmesi
- Yerli firmaların oluşturulmasıyla teknoloji maliyetlerinin düşürülmesi
- Güvenli server ve veri merkezlerinin oluşturulması, belirli standartların konularak ülke çapında bir standardın oturtulması

Endüstriyel Uygulamalar:

- Akıllı ağ (Smart Grid) teknolojisinin yaygınlaştırılması
- E-sağlık uygulamalarının artırılması ve kullanımının yaygınlaştırılması
- E-ticaret
    - İnternet üzerinden sipariş veren işletme sayısının internet kullanan işletme sayısına oranının artırılması
    - İnternet üzerinden sipariş veren bireysel kullanıcı sayısının internet kullanan bireysel kullanıcı sayısına oranının artırılması
    - İnternet bankacılığını kullanan bireysel kullanıcı sayısının internet kullanan bireysel kullanıcı sayısına oranının artırılması

- Akıllı ulaştırma
    - Telecommuting, akıllı trafik yönetimi gibi teknolojilerin gerçekleştirilmesi
- E-devlet altyapısı ve uygulamalarının geliştirilmesi

ÇİN

- Çin Halk Cumhuriyeti, siber güvenliğe dönük politikasının uygulanması için daha çok Çin ordusunun bünyesindeki kurumları yetkilendirmiştir. Türkiye'de siber güvenlik konusunda ana politika belirleyici seçilmiş hükümet olmakla birlikte, ordu-diğer kamu kurumları ve hükümet arasında yüksek düzeyli bir siber güvenlik istişare organı kurulması ve düzenli aralıklarla toplanarak dünyadaki ve Türkiye'ye dönük siber tehdit haritasına göre alınacak önlemlerin kararlaştırılması yararlı olacaktır. Çin özellikle ordusu bünyesinde yüksek sayıda siber güvenlik konusunda uzman personel çalıştırmaktadır ve bunun için 2 özel departman kurmuştur. Türk Silahlı Kuvvetleri bünyesinde de bir siber komutanlığın kurulması, gelecekte siber uzay üzerinden gelebilecek asimetrik tehditlerin karşılanması açısından da önemlidir.
- Buna ek olarak, Çin'in yaptığı gibi, sadece siber güvenlik üzerine çalışan ve teknoloji geliştiren AR-GE merkezlerinin kamu-özel işbirliği ile kurulması ve devlet tarafından güçlü şekilde desteklenmesi önemlidir.

ALMANYA

- Vatandaşlar ve küçük – orta ölçekli işletmeler tarafından kullanılan IT sistemleri için daha fazla güvenlik gerektiren altyapılar oluşturulmalıdır. Kullanıcılar, IT sistemlerinin kullanımı ile ilgili riskler ve güvenlik konusunda uygun ve tutarlı bilgi sahibi olmalıdırlar. Ortak girişimlerle beraber toplumu bilgilendirmek amacıyla bilgi havuzu oluşturulmalı ve birbiriyle tutarlı tavsiyeler devamlı olarak verilmelidir. Ayrıca devlet, bilgi sağlayıcıların sorumluluklarını denetleyerek, kullanıcılara sunulan temel bilginin,

uygun güvenlik ürünleri ve hizmetleriyle verildiğinden emin olacak. Devlet, temel güvenlik işlevleri için özel teşvikler ve fonlar sunmalıdır. IT sistemlerinin güvenli kullanımında küçük ve orta ölçekli işletmelerin desteklenmesi için Almanya örneğinde Ekonomi ve Teknoloji Federal Bakanlığı adı altında kurulan sanayinin katılımı ile IT güvenliği konusunda bir görev gücü kurulmuştur. Türkiye'de de buna benzer bir yapı oluşturulabilir.

- Bütün devlet makamları arasında operasyonel işbirliğinin oluşturulması ve IT olaylarından korunma ve müdahale önlemlerinin koordinasyonunu geliştirmek için bir Ulusal Siber Müdahale Merkezi kurulabilir. Almanya'da bu merkez, Bilgi Güvenliği Federal Dairesi, Anayasayı Koruma ve Sivil Koruma Federal Dairesi ve Afet Yardımı Federal Dairesi'ne rapor vererek doğrudan işbirliği yapacaktır. Ulusal Siber Müdahale Merkezi, ilgili tüm makamların yasal görevleri ve yetkilerine, sıkı işbirliği anlaşmaları temelinde uyacaktır. Federal Kriminal Dairesi (BKA), Federal Polis (BPOL), Gümrük Kriminolojik Ofisi (ZKA),Federal İstihbarat Servisi (BND), Alman Ordusu ve kritik altyapı işletmecileri denetleme makamlarının hepsi kendi kanuni görevleri ve yetkileri çerçevesinde bu çatı altında toplanmıştır.

- Eğer devlet siber saldırılara karşı tamamıyla hazırlıklı olmak istiyorsa siber saldırılara cevap vermek için koordineli ve kapsamlı bir araçlar bütünü, yetkili devlet makam ve mercilerinin işbirliği ile oluşturulmalıdır. Gerekli olması halinde, hükümet veya askeri düzeyde ilave kanuni yetkilerin yaratılması gerekip gerekmediği incelenmelidir.

ITU

1. **Hükümetin Siber Güvenlik için Sorumluluk Alması, Hesap Vermesi**

Ulusal bir siber güvenlik stratejisinin oluşturulması ve yerel, ulusal ve küresel sektörler arası işbirliğinin sağlanması konusunda hükümet sorumluluk almalıdır.

2. **Ulusal Siber Güvenlik Birimi**

Ülke içindeki siber güvenlik aktivitelerini bir kurum denetlemeli ve koordine etmelidir.

3. **Ulusal Siber Güvenlik Merkez Noktası**

Ülkenin her çeşit siber tehditten korunmasını ele alan tüm faaliyetler için merkez noktası olarak görev yapacak, birkaç ayrı ihtisas alanı biriminden oluşan bir kurum gereklidir.

4. **Hukuki Tedbirler**

Ceza mevzuatının (yasa, ikincil düzenlemeler vs.) siber suçlara cevap niteliğinde, caydırıcı ve cezalandırıcı hale getirilmesi için gözden geçirilmesi, güncellenmesi gereklidir.

5. **Ulusal Siber Güvenlik Çerçevesi**

Risk yönetimi ve mevzuata uyum gibi konularda asgari veya zorunlu güvenlik yükümlülükleri getirecek bir çerçeve oluşturulması gereklidir.

6. **Bilgisayar Olay Anında Müdahale Takımı**

Ulusal ölçekte sorumlu olacak bu yapı, siber tehditleri takip edecek, analiz edecek, tedbir ve olay anında müdahale stratejileri geliştirecek ve tüm paydaşlara bilgi verecektir.

7. **Siber Güvenlik Bilinçlendirme Çalışmaları ve Eğitim**

Siber tehditler hakkında bilinçlendirmeyi sağlayacak bir program şarttır.

8. **Kamu - Özel Sektör Siber Güvenlik Ortaklıkları**

Kamu ve özel sektörde anlamlı iş birlikleri yapılmalıdır.

9. **Siber Güvenlik Becerileri ve Beceri Kazandırma Programı**

Siber güvenlik uzmanları yetiştiren bir program başlatılmalıdır.

10. **Uluslararası İşbirliği**

Siber tehditlerin uluslar üstü etkileri sebebiyle ülkelerarası işbirliğine ihtiyaç duyulacağı aşikârdır.

BİRLEŞİK KRALLIK

1. Altyapının Korunması

Birleşik Krallık'ta, Ulusal Altyapının Korunması Merkezi (Center for the Protection of National Infrastructure), internet ve iletişim altyapıları da dahil olmak üzere ülkenin kritik altyapıların korunması konusunda çalışmakta; ilgili özel sektör altyapı kuruluşları ile devamlı iletişim halinde bulunmaktadır. Türkiye'de de internet ve iletişim altyapılarının korunması için ilgili özel sektör kuruluşları ile devamlı iletişim halinde olacak ve altyapıların korunması için bilgi alış verişinde bulunacak bir kuruluşun kurulması önemlidir.

2. Eğitim ve Araştırma

Birleşik Krallık, Ulusal Siber Güvenlik Programı çerçevesinde üniversitelerde siber güvenlik ile ilgili lisansüstü programlar geliştirme ve Birleşik Krallık'ın üç istihbarat ve güvenlik kuruluşundan biri olan GCHQ'nun yardımı ile siber güvenlik alanında bir araştırma merkezi kurma kararı almıştır. Geleceğin siber güvenlik uzmanlarının yetiştirilmesi ve siber güvenlik araştırmaları konusunda önde gelen ülkelerden biri olunması hususunda, üniversitelerde ilgili lisansüstü programlarının geliştirilmesi ve siber güvenlik alanında araştırma yapacak bir merkezin kurulması önemlidir.

AVRUPA BİRLİĞİ

- Mobil iletişimdeki güvenlik açıklarını takip ve tespit etmek için çalışma grupları oluşturulmalıdır.
- ENISA tarafında yürütülen siber güvenlik çalışmaları takip etmek ve uygulamalarda gözlemci olmak siber güvenlik ile ilgili uluslararası işbirliğinin geliştirilmesi açısından yararlı olacaktır.
- CERT projesiyle ilgili süreçlerin takibi ve en azından gözlemci seviyesinde bu oluşuma katılınması Türkiye Cumhuriyeti'nin siber güvenlikle mücadele tecrübesini arttıracaktır.

SİNGAPUR

- Siber güvenlik stratejisini hayata geçirmek için kurulması öngörülen idari birimin yasal çerçevesi belirlenirken, siber tehditlerin niteliği gereği ivedi bir şekilde karar alma ve uygulayabilmesine olanak tanıyacak bir yasal çerçevenin düşünülmesi gerekmektedir. Ayrıca kurulacak idari birimin kamusal siber güvenlik stratejileri ve uygulamaları arasında koordinasyonu sağlayabilmesi için söz konusu idari birimin kurucu kanununda tüm kamu kurum ve kuruluşların söz konusu idari birimin siber güvenlik ile ilgili kararlarına uymakla yükümlü olduklarına dair bir hüküm getirilebilir.

SITSA örneğinde olduğu gibi hem kamunun hem de özel sektörün Türk internet ağ altyapısına yönelik her türlü siber tehditle ilgili olarak bilgi paylaşımı yapabileceği ortak bir platform kurulmalıdır ve bu platformdaki her türlü paylaşımın en üst düzey gizlilik seviyesinde korunması sağlanmalıdır.