SİBER GÜVENLİK KURUMSAL YAPILANMASI: DÜNYA ÖRNEKLERİ VE TÜRKİYE İÇİN BİR KURUMSAL YAPILANMA ÖNERİSİ

Muhammed Raşit ÖZDAŞ*

ÖZET

Siber güvenliğin bireysel, kurumsal, ulusal ve küresel ölçekte önemi her geçen gün artmakta ve alınması gereken önlemlerde giderek daha karmaşık ve maliyetli hale gelmektedir. Günümüzde bilgi güvenliği, kurumlar arası olduğu kadar uluslararası işbirliklerini de gerekli kılan, yoğun yatay uzmanlık gerektiren, münferit projelerden ziyade ulusal çapta bütüncül bir bakış açısını zorunlu kılan bir hüviyet kazanmıştır. Bilişimin ülke ekonomilerinin ve kamusal süreçlerin en temel bileşenlerinden biri haline gelmesi ise siber güvenliği ulusal güvenlikle birlikte ele alan bir bakış açısının doğmasına sebep olmuştur. Bu doğrultuda, ülkeler ulusal siber güvenlik yapılanmalarını oluşturmakta ve böylelikle ulusal anlamda bütünleşik çözüm önerileri geliştirmeye çabalamaktadır. Ülkemizde de bu yönde bir eğilim söz konusu olup son dönemde yayımlanan ulusal siber güvenlik stratejileri çalışmalara bir ölçüde bütünlük kazandırmıştır. Bununla beraber, mevcut siber güvenlik kurumsal yapılanmasının kurumlar arası etkin işbirliğini sağlayacak özellikleri tam olarak taşımadığı değerlendirilmektedir. Bu çalışmada, siber güvenlik alanında ön planda yer alan ve coğrafi anlamda farklı özelliklere sahip olan ABD, Almanya, Güney Kore ve Japonya kurumsal siber güvenlik yapılanmaları açısından ele alınmış, Türkiye'nin mevcut durumu da incelenerek ülkemize ilişkin bir kurumsal yapılanma önerisi sunulmuştur.

Anahtar Kelimeler: siber güvenlik, kurumsal yapılanma, ABD, Almanya, Güney Kore, Japonya

INSTITUTIONAL STRUCTURE OF CYBERSECURITY: WORLD CASES AND AN INSTITUTIONAL STRUCTURE PROPOSAL FOR TURKEY

ABSTRACT

* Kalkınma Bakanlığı, Türkiye

The importance of cybersecurity increases everyday on individual, institutional, national, and global scope and required measures becomes even more complicated and costly. Nowadays, cybersecurity has become a field, which requires international cooperations along with national ones, complex and multi-disciplinary expertise, and nationwide comprehensive point-of-view instead of individual initiatives. After information technology became one of the most crucial components of national economies and public processes, a new approach showed up, strongly relating cybersecurity and national security with each other. With this respect, countries form their national cybersecurity institutional structurings and thus they struggle to develop integrated solution offers on a national scope. Such a tendency also exists in our country, since recently published national cybersecurity strategy documents provided unity in various efforts to some extent. On the other hand, existing cybersecurity institutional structuring does not fully satisfy effective cooperation needs among government institutions. In this study, countries remaining in the forefront of cybersecurity and having different geographic characteristics, which are United States of America, Germany, South Korea, and Japan, are analyzed in terms of cybersecurity institutional structurings, and current situation in Turkey has been examined along with a recommendation on national cybersecurity institutional structuring.

Keywords: cybersecurity, institutional structuring, USA, Germany, South Korea, Japan

GİRİŞ

Siber güvenliğin bireysel, kurumsal, ulusal ve küresel ölçekte önemi her geçen gün artmakta ve alınması gereken önlemler de giderek daha karmaşık ve maliyetli hale gelmektedir. Bilgisayarların boyut olarak küçülmesi ve yaygınlaşmasıyla birlikte bilgisayar güvenliği bağlamında ele alınan bilgi güvenliği, bilgisayarların birbirine bağlandığı bilişim sistemlerinin ortaya çıkmasıyla birlikte ağ güvenliği kapsamında değerlendirilmeye başlamıştır. İlerleyen süreçte internetin yaygınlaşması, bilişim sistemlerinin hayatın her alanında kullanılmaya başlaması, saldırı araçlarının ve yöntemlerinin nicelik ve nitelik itibarıyla artması gibi birbirini tamamlayıcı pek çok etmen sebebiyle karmaşık ve kuruluş seviyesinde alınacak önlemlerin yeterli olmayacağı bir sürece girilmiştir. Günümüzde bilgi güvenliği kurumlar arası olduğu kadar uluslararası işbirliklerini de gerekli kılan, yoğun yatay uzmanlık gerektiren, münferit projelerden ziyade ulusal çapta bütüncül bir bakış açısını zorunlu kılan bir hüviyet kazanmıştır. Bilişimin ülke ekonomilerinin ve kamusal süreçlerin en temel

bileşenlerinden biri haline gelmesi ise siber güvenlik ve ulusal güvenlik kavramlarının birlikte ele alınmasını sağlamıştır.

Başta ABD olmak üzere, tüm gelişmiş ülkelerde siber güvenliğe ilişkin bütüncül politikalar oluşturma gayreti söz konusudur. Ülkemizde de son dönemde benzer şekilde bir yaklaşım söz konusu olmuştur. Ancak ülkemizde süreç içerisinde mevcut kurumsal yapılanma çerçevesinde ele alınarak olgunlaştırılan yapının ne kadar etkin olduğu halen bir araştırma konusu olarak gündemdedir. Bu çalışmada, siber güvenlik alanında önde gelen bazı ülkelerin kurumsal yapılanmaları incelenerek ülkemiz için bir kurumsal yapılanma önerisi sunulmaktadır.

Çalışma kapsamında Amerika Birleşik Devletleri (ABD), Almanya, Güney Kore ve Japonya ülkeleri incelenmiştir. Ülkelerin seçilmesinde temel olarak siber güvenlik alanındaki olgunluk seviyesi dikkate alınmış olup coğrafi çeşitliliğe de önem verilmiştir. İncelenmiş olan tüm ülkeler, güvenilir kaynaklar tarafından yapılmış dünya sıralamalarında ilk 10'da yer almaktadır.[111] Bölgesel çeşitlilik bağlamında, Avrupa Birliği ülkelerinden Almanya, uzak doğu ülkelerinden ise Japonya ve Güney Kore seçilmiştir. Güney Kore'nin incelenmesinin bir diğer sebebi ise, yakın dönemde farklılaşmış olmakla birlikte, sahip olduğu çok sayıda göstergenin ülkemizi yansıtır nitelikte olmasıdır.

Çalışma kapsamında, ilk bölümde ülkelerin kurumsal yapılanmaları ele alınmakta, ikinci bölümde Türkiye'deki mevcut durum aynı kapsamda analiz edilmekte ve son bölümde Türkiye için bir siber güvenlik kurumsal yapılanma önerisi sunulmaktadır.

BAZI ÜLKELERDE SİBER GÜVENLİĞİN KURUMSAL YAPILANMASI

Bu bölümde siber alanında gelişmiş ABD, Almanya, G. Kore ve Japonya'nın siber güvenlik kurumsal yapılanmaları kısaca gözden geçirilecektir.

Amerika Birleşik Devletleri (ABD)

ABD'nin siber güvenlik kurumsal yapılanması Şekil 1'de gösterilmektedir. Kamu kurum ve kuruluşları kendi güvenliklerini sağlamak ve ilgili mevzuata uymakla, regülasyon kurumları

[11] Bahsi geçen sıralamalara örnek olarak, Uluslararası Telekomünikasyon Birliği (International Telecommunications Union, ITU) tarafından 2014 yılında yayınlanan Küresel Siber Güvenlik Endeksi ile dünyaca ünlü bir araştırma kuruluşu olan Booz-Allen-Hamilton tarafından 2011 yılında yapılan Siber Güç Endeksi verilebilir.

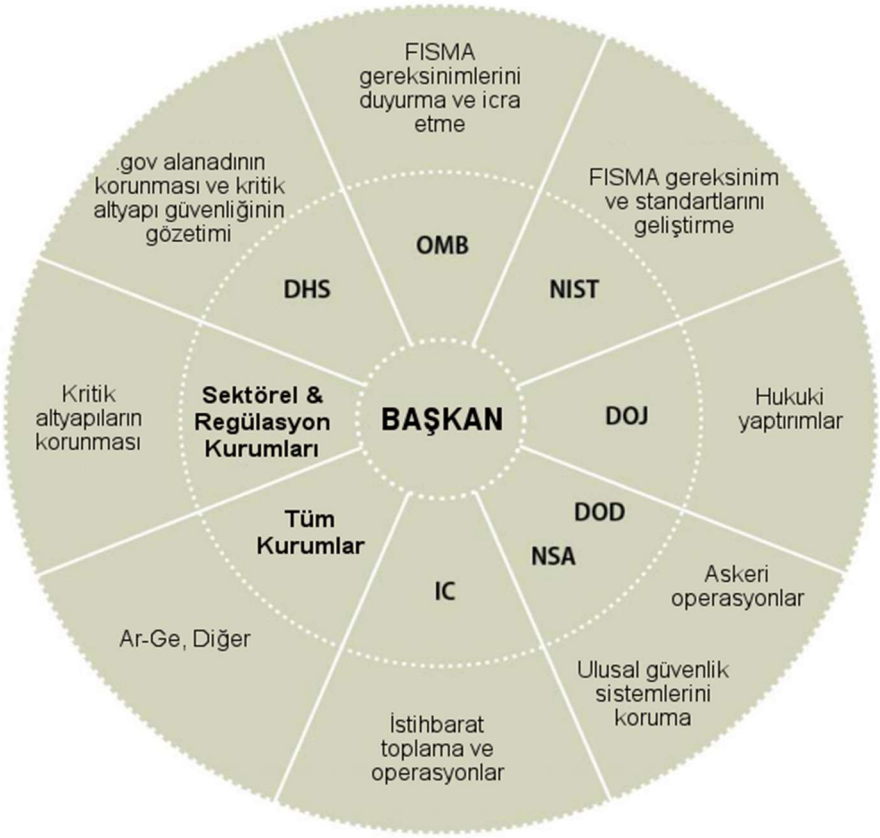
ise kendi güvenlikleriyle birlikte hükmü altındaki kuruluşların güvenliğini temin edecek yaptırımları hayata geçirmekle yükümlüdür. Bu kurumlar yetkileri oranında zorunlu veya isteğe bağlı girişimler hayata geçirmektedir (Daniel, 2014).

Ulusal Güvenlik Konseyi (National Security Council, NSC). Beyaz Saray bünyesinde faaliyet gösteren Konsey, ABD başkanının ulusal güvenlik ve dış politika konularıyla ilgili konularda birincil organıdır. Başkan tarafından yönetilen, bakanlar ve diğer üst düzey temsilcilerin katılım sağladığı konseyin temel görevi ilgili konularda Başkan'a danışmanlık hizmeti sunmaktır. Konseyin iki temel çalışma alanıyla da ilişkili olması sebebiyle, siber güvenlik öncelikli çalışma konuları arasında yer almaktadır (White House, t.y.).

Bilgi ve İletişim Altyapısı Kurumlar Arası Politika Komitesi (Information and Communications Infrastructure Interagency Policy Committee, ICI-IPC). Ulusal Güvenlik Konseyine bağlı bir komite olan ICI-IPC, politika seviyesinde en önemli kamu aktörü olup siber güvenlik çalışmalarında stratejik düzeyde koordinasyon görevi üstlenmektedir.

Anayurt Güvenliği Bakanlığı (Department of Homeland Security, DHS). Siber güvenlik alanındaki çalışmaların koordine edilmesi amacıyla 2002 yılında Anayurt Güvenliği Kanunu ile kurulan DHS, Federal Bilgi Sistemleri Yönetimi Kanununun (FISMA) 2014'te güncellenmesiyle birlikte ulusal koordinasyon gücünü artırmıştır. Kurumun ana görevi federal bilgi sistemlerinin ve kritik altyapıların korunmasıdır. Bu görevlerin etkin şekilde gerçekleştirilebilmesini temin etmek amacıyla son yıllarda özellikle kamu-özel sektör arasındaki bilgi alışverişine ağırlık verilmiştir. DHS ve NSA işbirliğiyle 2000'li yılların başından beri ülke genelinde üniversitelerin siber güvenlik alanındaki programları akredite edilmektedir. DHS ile Savunma Bakanlığı (DoD) arasında görev paylaşımı ve yetki seviyesi açısından bir belirsizlik söz konusudur (Murray, Zeadally ve Flowers, 2012:289). Mevcut durumda 16 farklı kritik altyapı sektörü belirlenmiş olup bunlar; kimyasal tesisler, ticari tesisler, iletişim, kritik üretim, barajlar, endüstriyel savunma üssü, acil durum hizmetleri, enerji, finansal hizmetler, gıda ve tarım, kamu tesisleri, sağlık hizmetleri ve kamu sağlığı, bilgi teknolojileri, nükleer reaktörler, materyaller ve atık, ulaşım sistemleri, su ve atık su sistemleridir (White House, 2013). DHS bünyesindeki 7/24 aktif faaliyet yürüten bir merkez aracılığıyla DHS'nin diğer kurumlar ve kritik altyapı işletmecisi kuruluşlar arasındaki anlık bilgi paylaşımı sağlanmaktadır (DHS, 2016).

Şekil 1. ABD'deki Siber Güvenlik Kurumsal Yapılanması



Kaynak: Fischer, 2012

Yönetim ve Bütçe Ofisi (Office of Management and Budget, OMB). Beyaz Saray'a bağlı olan Ofis 2014 yılında FISMA'nın federal seviyede uygulanmasından sorumlu kuruluş olarak belirlenmiştir (U.S. Congress, 2014). DHS ile yakın işbirliği içerisinde olan Ofis, bütçeyi elinde bulundurması sebebiyle kuruluşlara harcamalar konusunda esneklik sağlayabilmekte ve olası mali engellerin kısa sürede aşılmasını sağlayabilmektedir.

Adalet Bakanlığı (Department of Justice, DoJ). Bakanlık siber güvenlik mevzuatına ilişkin yaptırımların yürütülmesinden sorumludur. Bilişim suçlarıyla mücadelenin yanı sıra diğer kamu kurumlarına hukuki anlamda destek faaliyetleri de yürütmektedir (U.S. Department of Justice, 2013). 2006 yılında Adalet Bakanlığı tarafından yerel mahkemelerde Bilgisayar Suçları ve Telif Hakları Bölümü oluşturulmuştur. Bu birim, avukatlara bilişim suçlarını anlama ve doğru değerlendirme konusunda destek olmaktadır (Ferwerda, Choucri ve Madnick, 2010). Bu birim altında 2014 yılında kurulan Siber Güvenlik Birimi bu alanda hızla değişen tehdit türlerine karşı mevzuatın daha etkin ve hızlı bir şekilde güncellenebilmesini amaçlamaktadır (U.S. Department of Justice, 2016). Başkanlık sisteminin getirdiği esnek ve

etkin yönetim avantajına rağmen hızla değişen tehdit türlerine karşı yeterli aksiyonun alınamıyor olduğu gözlenmekte, bu durum kuruluş tarafından yayınlanan raporlarda da yer almaktadır.[12]

Savunma Bakanlığı (Department of Defense, DoD). Anayurt Güvenliği Bakanlığının ".gov" uzantılı alan adlarını korumasına benzer şekilde, Savunma Bakanlığı ".mil" uzantılı askeri alan adlarını korumakta, ayrıca küresel çapta askeri bilgi sistemlerini ve üsleri güvenlik altına almaktadır. Bakanlık bu amaçla siber tehdit verilerini toplar. Bakanlık bünyesindeki Siber Güvenlik Komutanlığı koordinasyonunda operasyonel seviyedeki faaliyetler yürütülmektedir.

İleri Savunma Araştırma Projeleri Ajansı (Defence Advanced Research Projects Agency, DARPA). Savunma Bakanlığına bağlı askeri bir kuruluş olan DARPA, Ar-Ge projeleri yürütmektedir. Proje geliştirme süreçlerinde kamu kurumları ve özel sektörle yakın işbirliği içerisinde olan DARPA'da Ağustos 2016 itibarıyla savunma alanında yaklaşık 250 aktif proje bulunmaktadır (DARPA, t.y.). Kuruluş personel sayısı 500'ün altında olup projeler ihale ya da ikili işbirliği usulüyle sürdürülmektedir. Kuruluş genel itibarıyla özel sektör tarafından üstlenilmesi fayda-maliyet anlamında pratik olmayacak projeleri üstlenip özel sektör tarafından geliştirilmeye devam edilebilecek noktaya gelindiğinde özel girişimlere devretme prensibiyle çalışmaktadır. DARPA tarafından belirli konularda yarışmalar da düzenlenmektedir. Örneğin sürücüsüz araçlara ilişkin 2004 yılında düzenlenen yarışmanın hiç kazananı olmasa da sonraki yıllarda özel sektör yatırımlarının bu alana kaymasını ve günümüzde bu alanın ciddi bir ekonomik avantaj olarak ortaya çıkmasına zemin hazırlamıştır (Thompson, 2015).

İstihbarat Teşkilatı (Intelligence Community, IC). İstihbarat teşkilatı 16 kuruluşun üye olduğu, Beyaz Saray'a bağlı Ulusal İstihbarat Başkanınca yönetilen bir teşkilattır. Üyeleri arasında Merkezi İstihbarat Kurumu (CIA), Federal Soruşturma Bürosu (FBI), Ulusal Güvenlik Ajansı (NSA), Ulusal Mekansal İstihbarat Ajansı, Savunma İstihbarat Ajansı ve Sahil Koruma İstihbaratı gibi istihbarat kuruluşlarının yanı sıra Enerji Bakanlığı, Anayurt Güvenliği Bakanlığı, Hazine Bakanlığı gibi bakanlıklar da yer almaktadır. (DNI, t.y.)

[12] Kuruluş tarafından her yıl yayınlanan "Adalet Bakanlığının Karşılaştığı En Önemli Yönetim ve Performans Zorlukları " raporunun 2016 sayısında siber güvenliğe 9 zorluk arasında 2. sırada yer verilmiştir. (Horowitz, 2016)

Merkezi İstihbarat Kurumu (Central Intelligence Agency, CIA). Kuruluşun temel görevi üst düzey ABD kurumlarına ve yetkililerine istihbarat sağlamaktır. Bağımsız bir kuruluş olan CIA'in yöneticisi, ABD Başkanının önerisi ve Senato'nun kararı ile atanmaktadır.

Ulusal Güvenlik Ajansı (National Security Agency, NSA). Çok sayıda şifreleme uzmanının çalıştığı Ajans, ABD kurumları arasındaki iletişimin güvenliğini sağlamak ve dünya genelinde şifreli iletişime ilişkin istihbari faaliyetlerde bulunmakla görevlidir. Savunma Bakanlığına bağlı olan Ajansın dünyanın pek çok farklı ülkesinde aktif çalışanı bulunmaktadır. (NSA, 2016)

Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology, NIST). Ticaret Bakanlığına bağlı olan kuruluş, geniş bir yelpazede teknik standartlar geliştirmektedir. Siber güvenliğin artan önemiyle birlikte kuruluş bu alanda da faaliyet göstermeye başlamış olup çalışmaları dünya genelinde takip edilmektedir. Siber güvenlik alanında işgücü ihtiyacının ciddi şekilde artmasıyla birlikte kuruluş eğitim faaliyetlerinde de aktif rol üstlenmeye başlamıştır. Örneğin NIST öncülüğünde yürütülmekte olan Siber Güvenlik Eğitimi için Ulusal Girişim (National Initiative for Cybersecurity Education, NICE) programı ile ilgili tüm tarafların bir araya getirildiği bir işbirliği ortamı oluşturulmuştur. (NICE, t.y.).

Federal Ticaret Komisyonu (Federal Trade Commission, FTC). Bu komisyon vatandaşların ticari anlamda korunmasına ve etkin rekabet ortamının oluşturulmasına yönelik görevler icra etmekte olup son yıllarda veri mahremiyeti alanında da faaliyet göstermeye başlamıştır. Özel sektör kuruluşlarına yönelik hukuki düzenlemeler yayımlayan komisyon, çevrimiçi alışveriş yapan çocukların kişisel verilerinin korunmasına özellikle önem vermektedir. (FTC, 2016).

Internet Suç Şikâyet Merkezi (Internet Crime Complaint Center, IC3). Merkez, 2001 yılında FBI ile Ulusal Beyaz Yaka Suç Şikayet Merkezi işbirliği ile kurulmuştur. İnternet suçlarının bildirilmesi için merkezi nokta hüviyetindedir. İnternet suçlarının büyük oranda raporlanmadığı ve IC3'e ulaşan şikayetlerin toplam içerisinde düşük bir yüzdeye sahip olduğu belirtilmektedir. (IC3, 2008).

Ulusal Siber Olaylara Müdahale Ekibi (SOME) Yapılanması. Carnegie Mellon Üniversitesi Yazılım Mühendisliği Enstitüsü (SEI) bünyesinde yer alan SOME'nin koordinasyonunda ülkede 72 adet SOME faaliyet göstermektedir. Bunlardan 56 tanesi (%78) özel sektör

kuruluşlarına, 5 tanesi üniversitelere, 5'i kamuya ve 6 tanesi de ulusal ve uluslararası STK'lara aittir. Bu anlamda ABD SOME yapılanması içerisinde özel sektör ağırlığının oldukça fazla olduğu göze çarpmaktadır. SOME'ler arası koordinasyon ise kamu eliyle yürütülmektedir. Küresel çapta faaliyet gösteren neredeyse bütün firmaların SOME yapılanması mevcut olup bunlar bu alanda otorite sayılan Olay Müdahale ve Güvenlik Ekipleri Forumu (FIRST) kuruluşuna da üyedir. Özellikle güvenlik çözümü geliştiren firmalardan küresel çapta faaliyet göstermeyenler de FIRST üyesidir. Bunların yanı sıra Ulusal Havacılık ve Uzay Dairesi (NASA), Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) gibi kuruluşlar da FIRST üyesi kamu kuruluşlarıdır. Kamu kuruluşlarının federal seviyede SOME koordinasyonuna yönelik çalışmalar US-CERT adında bir SOME yapılanması tarafından yürütülmektedir. Belirli bir organizasyonu koruma amaçlı kurulan SOME'ler olduğu gibi, siber güvenliğin bir alanında uzmanlaşmış olan ve bu yönüyle ihtiyaç duyan tüm kuruluşlara hizmet veren SOME'ler de bulunmaktadır.

Almanya

Almanya siber güvenlik yapılanmasında BSI en etkin ve öne çıkan kuruluştur. Koordinasyon, denetim, eğitim gibi siber güvenliğin yatay eksendeki hemen hemen tüm alanlarının koordinasyon ve denetiminden BSI sorumludur. Bunun yanı sıra tüm kamu kurum ve kuruluşları kendi güvenliklerini sağlamakla, regülasyon kuruluşları buna ilave olarak etki alanına giren kuruluşların da güvenliğini temin edecek yaptırımları hayata geçirmekle yükümlüdür.

Federal Bilgi Güvenliği Ofisi (Bundesamt für Sicherheit in der Infromationstechnik, BSI).

İçişleri Bakanlığı gözetimi ve denetimi altında faaliyet gösteren BSI'ın başlıca görevleri arasında federal bilgi sistemlerine yönelik tehditleri önlemek, kamu kurumlarıyla bilgi ve tecrübe paylaşımında bulunmak, standart, test ve sertifikasyon mekanizmalarını hayata geçirmek, kritik altyapıların korunmasına ilişkin önlemleri almak ve aldırmak, özel sektörle işbirlikleri oluşturmak, kamuda çalışan insan kaynağının bu alanda gelişimini desteklemek gibi faaliyetler yer almaktadır.

Yerel yazılım üretilmesi çalışmaları kapsamında özellikle kritik uygulamalarda gereksinim duyulan şifreleme cihaz ve yazılımlarının geliştirilmesi BSI tarafından bizzat yürütülmektedir. BSI istihbarat, polis birimleri ve savcılık gibi güvenlik birimleriyle daha yakın işbirliği ile çalışmaktadır. Federal bilgi sistemlerine yönelik standartlar BSI tarafından hazırlanarak İçişleri Bakanlığına sunulmakta, Bakanlık bu standartları zorunlu tutmaktadır. Ancak tek bir

bakanlığın sorumluluğu altında olmayan veya uygulanması bakanlıklar arası işbirliğini gerektiren standartlar bakanlar kurulu kararı olarak hayata geçirilmektedir (BSI, 2009). Özel sektörle yapılan ortak çalışmalar ve bilgi alışverişi faaliyetleri kapsamında, Federal Bilgi Teknolojileri, Telekomünikasyon ve Yeni Medya Birliğinin (BITKOM) de desteğiyle gönüllülük esasına dayanan Siber Güvenlik Birliği oluşturulmuştur. Kamu, özel sektör ve üniversitelerden temsilcilerle birlikte 2.300 civarında firmanın katılım sağladığı birliğin temel görevi kamu ve özel sektör işbirliğinin sağlanması ve siber olayların etkin bir şekilde duyurulmasıdır (ACS, t.y.; BITKOM, t.y.).

Almanya'da ulusal bir siber güvenlik konseyi kurulmasına yönelik çalışmalara Şubat 2011'de hayata geçen Almanya Siber Güvenlik Stratejisinde 10 temel öncelikten biri olarak yer verilmiştir (BMI, 2011). Yapılan çalışmalar neticesinde operasyonel bir birim olan Ulusal Siber Savunma Merkezi kurulmuş, ancak politik kararlar alabilecek seviyede bir konsey henüz hayata geçmemiştir.

Federal Temsilcilikler. Almanya'da Federal temsilciliklerle politika seviyesinde koordinasyon sağlanmaktadır. Bu temsilcilikler çalıştıkları konuya göre başbakan veya bakan tarafından geçici veya sürekli olarak oluşturulabilmektedir. (BSI, t.y.)

2009 yılında yayımlanan Federal Veri Koruma Kanunu ile Federal Veri Koruma ve Bilgi Özgürlüğü Temsilciliği oluşturulmuş ve Ocak 2016'da bağımsız bir düzenleyici kuruluş halini almıştır (BfDI, t.y.). Bu birim, telekomünikasyon ve posta hizmeti sunan kuruluşların denetimi ile kamu kurumlarının veri toplama faaliyetlerinin denetimini yapmaktadır.

Siber güvenlik alanında kısmi surette de olsa faaliyet gösteren bir temsilcilik olan Federal Bilgi Teknolojileri Temsilciliği ülke çapında bilgi teknolojileri projelerine ilişkin koordinasyon, tanıtım ve denetim faaliyetleri yürütmektedir. (BMI, t.y.)

Ulusal Siber Savunma Merkezi (Nationales Cyber-Abwehrzentrum). Almanya İçişleri Bakanlığı tarafından Haziran 2011'de oluşturulan merkez, BSI nezaretinde faaliyet göstermektedir. Almanya siber savunma stratejisinde en öncelikli olarak ele alınan husus kritik altyapıların güvenliğidir. Bu nedenle kurulan bu merkezin en temel görevi, ulusal çapta etkiye sahip bilgi güvenliği olaylarını hızlı ve kapsamlı bir şekilde değerlendirip alınacak karşı önlemlere ilişkin koordinasyonu sağlayacak önerilerde bulunmaktır (Hunton & Williams LLP, 2011). Merkez operasyonel seviyede görevler üstlenmiştir.

Federal Ağ Altyapısı Ajansı (Bundesnetzagentur). Bu kuruluş telekomünikasyon alanındaki düzenlemeleri hayata geçirmenin yanı sıra elektronik imza kök sertifikalarının temininden de sorumludur. (Bundesnetzagentur, t.y.)

Almanya'da Kamuya ait SOME Yapılanması. Almanya'da ulusal çapta faaliyet gösteren, resmi olarak yetkilendirilmiş SOME kuruluşu CERT-Bund'dur. Her ülkede benzer nitelikte yürütülen SOME faaliyetlerine ek olarak, Ulusal Bilgi Teknolojileri Durum Merkezi de bu birim tarafından yürütülmektedir. (CERT-Bund, t.y.)

Federal Sivil Savunma ve Afet Kurtarma Ofisi (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK). Bu kuruluş afet ve acil durum önlemleri alanında faaliyet göstermekte olup başta kritik altyapıların korunması olmak üzere siber güvenlik alanındaki faaliyetlerde BSI ile işbirliği içerisinde çalışmaktadır. Bu işbirliği kapsamında hayata geçirilen ulusal çapta önemli girişimlerden bir tanesi UP KRITIS girişimidir. Bu girişim, kritik altyapıların korunması alanında kamu - özel sektör işbirliğini temin etmek amacıyla hayata geçirilmiştir. (UP KRITIS, t.y.)

Federal İstihbarat Servisi (Bundesnachrichtendienst, BND). İkinci dünya savaşının ardından kurulmuş olan birimin temel amacı ulusal güvenlik politikalarını etkileyebilecek tüm bilgilerin bir merkezde toplanması ve karar destek mekanizması amacıyla kullanılmasıdır (BND, t.y.). Kuruluş, diğer ülkelerdeki istihbarat servislerine benzer bir görev üstlenmiştir.

Ekonomi ve Teknoloji Bakanlığı (Bundesministerium für Wirtschaft und Energie). Bakanlık, BSI tarafından hazırlanan rehber ve standartlardan da faydalanmak suretiyle özel sektörde bilgi güvenliği farkındalığının artması için rehberlik ve destek faaliyetleri yürütmektedir (BWE, t.y.) Bakanlık bu amaçla bir "task force" oluşturmuştur. (BMI, 2011) .

İnternet Şikâyet Ofisi (Internet-beschwerdestelle). Gönüllülük esasına dayalı bir sivil toplum kuruluşu olarak faaliyet gösteren bu ofis, internet kullanımına yönelik şikayetleri alarak ilgili kişi, kurum veya kuruluşlara ulaştırmaktadır. Almanya İnternette Güvende girişiminin bir parçası olarak faaliyet göstermektedir. (Internet-Beschwerdestelle, t.y.)

Güney Kore

Başkanlık Siber Güvenlik Ofisi. Gittikçe artan Kuzey Kore siber saldırılarına daha etkin bir şekilde karşı koyabilmek amacıyla Mart 2015'te Başkanlık bünyesinde bir Siber Güvenlik Ofisi kurulmuştur (Byrne, 2015). Ancak Başkanlık web sitesi incelendiğinde bu yapının

görünür olmadığı ve uzun vadeli olarak tasarlanmadığı, Kuzey Kore tehditi kapsamında geçici bir çözüm olarak ele alındığı anlaşılmaktadır.

Kore İletişim Komisyonu. Komisyonun esas sorumluluk alanı yayıncılık sektörünün regülasyonu olmakla birlikte, zaman içinde telekomünikasyon ve yayıncılık sektörlerinin birbirine yakınsaması sebebiyle telekomünikasyon sektörünün regülasyonuyla ilgili de faaliyet yürütmeye başlamıştır (KCC, t.y.). Bu hizmetleri tamamlayıcı olarak, ilgili olduğu sektörlere ilişkin siber güvenlik alanında stratejiler ve eylem planları hazırlamaktadır. Komisyona veri mahremiyetini destekleyici nitelikte yazılım geliştirip dağıtımını yapma hakkı da kanunen tanınmıştır (PPC, 2015). Komisyon tarafından hazırlanan politika dokümanlarının takip ve denetimini Ulusal İstihbarat Servisi yapmaktadır (NIS, t.y.).

Kore İletişim Standartları Komisyonu. Komisyonun temel görevi, telekomünikasyon işletmecilerinin kaynakların adil kullanımı ilkesi gereğince regüle edilmesini sağlamaktır. Komisyon bu temel görevin yanı sıra çevrimiçi verilerin güvenliği konusunda da çalışmalar yürütmektedir. Komisyon bünyesinde faaliyet gösteren Yasadışı ve Zararlı Bilgi İhbar Merkezi aracılığıyla internetin güvenli kullanımı hedeflenmiş, ayrıca internet servis sağlayıcılarının işbirliğiyle oluşturulmuş online içerik derecelendirme sistemi ile ebeveynlerin ve öğretmenlerin çevrimiçi içeriği derecelendirmeleri imkânı sunulmuştur (KCSC, t.y.).

Bilim, Bilgi ve İletişim Teknolojileri ve Gelecek Planlaması Bakanlığı. Temel görevi genel anlamda BİT teknolojilerine ilişkin politika oluşturmak olan kuruluş, siber güvenliğe ilişkin politika seviyesinde ve operasyonel seviyede çalışmalar da yürütmektedir. Bakanlık bünyesinde bulunan BİT Politikaları Ofisi altında yer alan Siber Güvenlik Politika Bürosu hem politika oluşturma hem de operasyonel seviyede faaliyetler yürütmekten sorumludur (MSIP, t.y.). Bakanlığın organizasyon yapısına bakıldığında, siber güvenliğin yönetim seviyesinde ele alınan bir husus olmadığı gözlenmektedir.

Kişisel Verileri Koruma Komisyonu. Eylül 2001'de Kişisel Verileri Koruma Kanunu ile kurulmuş olan Komisyon, doğrudan Başkanlığa bağlı özerk bir yapıdır. Komisyonun temel görevi, vatandaşların kişisel verilerinin amacına uygun toplanması ve mahremiyet ihlallerine sebebiyet verilmemesine ilişkin çalışmalar yürütmektir (PPC, t.y.b).

Kore İnternet ve Güvenlik Ajansı. Ajansın temel görevleri internetin desteklenmesi, bu alanda ulusal ve uluslararası işbirlikleri ve internet güvenliğinin sağlanmasıdır. Ülkenin siber güvenlik alanında teknik anlamda yetkin bir kuruluşu olup Kore İletişim Komisyonu altında

faaliyet göstermektedir (KISA, t.y.). Kuruluş tarafından siber güvenlik alanında ulusal çerçeve oluşturacak nitelikte çalışmalar yürütülmektedir. Kuruluş ayrıca Bilim, Bilgi ve İletişim Teknolojileri ve Gelecek Planlaması Bakanlığı tarafından kendisine verilen operasyonel görevleri yürümekle ve gelişmeleri periyodik olarak Bakanlığa raporlamakla yükümlüdür (PPC, 2015). Ülkenin vatandaşlara ve kuruluşlara yönelik SOME yapılanması bu kuruluşa bağlı olarak faaliyet göstermektedir.

Ulusal İstihbarat Servisi. Ülkenin istihbarat kuruluşu olan bu birim, siber güvenlik alanında kamuya operasyonel seviyede öncülük etmektedir. İlgili kuruluşlarca hazırlanan siber güvenlik politikalarının denetim ve takibini yapar. Ayrıca kuruluşların kendi yetkinlikleriyle altından kalkamayacakları sorumluluklarda onlara teknik destek vermektedir (NIS, t.y.).

Güney Kore SOME Yapılanması. Ulusal seviyede siber olaylara müdahale koordinasyonunu sağlayan kuruluş KrCERT/CC kuruluşudur. Kore İnternet ve Güvenlik Ajansına bağlı olarak faaliyet gösteren bu birim genel olarak vatandaş, özel sektör ve sivil toplum kuruluşlarına yönelik faaliyet yürütmektedir. Bu kuruluş, uluslararası bağlamda ülkenin operasyonel temas noktasıdır. Kamu kurumlarının siber alanda korunmasıyla ilgili koordinasyon görevi ise diğer bir ulusal SOME yapılanması olan ve Ulusal İstihbarat Servisi altında faaliyet gösteren KN-CERT kuruluşuna verilmiştir (BSA, 2015b).

Ulusal Siber Komutanlığı. Askeri kuvvetlere bağlı bu birim, askeri alanda siber saldırılara müdahale ve karşı önlemler almakla yükümlüdür.

Japonya

Japonya'da siber güvenlik 2004 yılında stratejik seviyede ele alınmaya başlamış olup 2005 yılında Bilgi Güvenliği Politikası Komisyonu ile Ulusal Bilgi Güvenliği Merkezi kurulmuştur (NISC, 2007).

Bilgi Teknolojileri Stratejik Genel Merkezi. Uzun adı Gelişmiş Bilgi ve Telekomünikasyon Şebekesi Toplumunun Teşviki için Stratejik Genel Merkez olan birim, Bakanlar Kurulu bünyesinde Ocak 2001'de kurulmuştur (Japan Cabinet, 2000). Birim bilgi teknolojilerine ilişkin stratejik kararların alındığı ve politikaların belirlendiği, ülkenin en üst düzey oluşumudur.

Bilgi Güvenliği Politikası Komisyonu. 2004 yılında gerçekleşen kurumsal gözden geçirme çalışmaları sonucunda Bilgi Teknolojileri Stratejik Genel Merkezi bünyesinde kurulan komisyon, siber güvenlik alanında ulusal çapta stratejik kararların alınmasından sorumludur. Ayrıca bilgi güvenliği alanında kamu kurumlarının uyması gereken asgari standartların geliştirilmesinden de bu komisyon sorumludur (NISC, 2007).

Ulusal Güvenlik Konseyi. Konsey, genel anlamda ulusal güvenlikten sorumlu olup, siber güveniğe ilişkin hususlarda Bilgi Güvenliği Politikası Komisyonu ile yakın işbirliği içerisinde çalışmaktadır (BSA, 2015a).

Ulusal Bilgi Güvenliği Merkezi. 2004 yılında gerçekleşen kurumsal gözden geçirme çalışmaları sonucunda Bilgi Teknolojileri Stratejik Genel Merkezi bünyesinde kurulan Merkez, üst seviyede alınan politika kararlarının operasyonel seviyede uygulanması ve koordinasyonundan sorumlu olup faaliyetlerini kamu ve özel sektörden uzmanların geçici görevlendirilmesi suretiyle yürütmektedir. Merkez operasyonel anlamda siber güvenlik alanında teknik seviyede stratejilerin oluşturulması, yeni teknolojilerin takibi, ar-ge, kamu kurumlarında bilgi güvenliği analiz ve değerlendirmesi, kritik altyapıların korunması gibi işlevler üstlenmektedir. Merkez, çalışmalarını periyodik olarak Bilgi Güvenliği Politikası Komisyonuna sunar ve komisyon, bu merkezden aldığı verilere dayanarak yıllık plan ve ulusal strateji belgeleri hazırlar. Komisyon tarafından kamu kurumlarına zorunlu tutulan asgari standartların denetim ve takibini yapmaktan ve rehberler hazırlamaktan da bu merkez sorumludur (NISC, 2007).

Kişisel Verileri Koruma Komisyonu. Daha önceden var olan Özellikli Kişisel Verileri Koruma Komisyonu adı ve kapsamı değiştirilerek mevcut halini almıştır. Komisyon başkanı ve üyeleri 5 yıl süreyle meclisin onayıyla Başbakan tarafından atanmaktadır. Komisyon üst kurul niteliğinde olup özerk bir yapıdadır. Özel sektör kuruluşlarını kişisel verileri koruma organizasyonu olarak yetkilendirmekte ve kendisine ulaştırılan şikâyetleri bu yetkilendirilmiş üçüncü taraflar aracılığıyla çözüme kavuşturmaktadır (PPC, t.y.a).

Müşteri İlişkileri Ajansı. Ajans, Kişisel Verilerin Korunması Kanunu kapsamındaki yaptırımların uygulanmasında merkezi otorite kuruluş olarak adlandırılabilir. Bununla birlikte tüm bakanlıkların sorumlu olduğu sektörlere ilişkin yaptırım ve yönlendirme gücü bulunmaktadır (Raul, Manoranjan ve Mohan, 2014).

Bilgi Teknolojileri Teşvik Ajansı. Kuruluş, insan kaynağı geliştirilmesi, bilgi güvenliği ve bilgi sistemlerinin güvenilirliğinin (bel bağlanabilirliğinin) artırılması olmak üzere üç temel alanda faaliyet göstermektedir (IPA, t.y.). Bilgi güvenliğinin en temel üç faaliyet alanından biri olmasının sebebi, bilgi teknolojilerine bağlı ekonomik kalkınmanın etkin güvenlik tedbirlerine sıkı sıkıya bağlı oluşunun içselleştirilmiş olmasıdır. Kuruluş genel anlamda özel sektörün teşvik edilmesi odağında bilgi teknolojileri politikaları hazırlamaktadır.

JPCERT Koordinasyon Merkezi. 1996 yılında kurulmuş olan ve kısa adı JPCERT/CC olan merkez, ulusal SOME yapılanmasının koordinasyonundan sorumludur. Ayrıca Asya - Pasifik bölgesinin bölgesel SOME yapılanması olan Asya-Pasifik Bilgisayar Olaylarına Müdahale Ekibi (APCERT, t.y.) oluşumunda öncül bir rol üstlenmekte olup sekreterya vazifesi de görmektedir. APCERT'e ait internet sitesi dahi JPCERT/CC tarafından yönetilmektedir (JPCERT/CC, t.y.).

Japonya Şebeke Güvenliği Birliği. Özel sektör kuruluşlarının katılım sağladığı birlik, telekomünikasyon şebekelerinde güvenlik standardizasyonu ağırlıklı olmak üzere teknik alanda standartların geliştirilmesi ve uygulanmasına yönelik faaliyetler yürütmektedir (JNSA, t.y.).

Savunma Sektörü Kuruluşları. Savunma alanında faaliyet gösteren kuruluşların önde gelenleri Polis kuvvetlerinin yönetiminden sorumlu Ulusal Polis Ajansı, ulusal savunma alanında faaliyet gösteren Savunma Bakanlığı, istihbarat faaliyetlerinden sorumlu Kamu Güvenlik İstihbarat Ajansıdır.

Ülke Örneklerinin Genel Değerlendirmesi

İncelenen ülkelere genel olarak bakıldığında, siber güvenlik alanındaki bilgi ve tecrübe birikiminin en yoğun şekilde ABD'de olduğu gözlenmektedir. Ülkeler siber güvenlik politikalarını etkinleştirme yolunda temel bazı evrelerden geçmiştir. Bu evreler kabaca şu şekilde listelenebilir:

1. Kurumların münferit çabaları ve merkezi kuruluşların rehberlik niteliğinde yönlendirmeleri
2. Otorite kuruluşlar oluşturulması, strateji ve politikalarla ulusal yönelimin belirlenmesi
3. Merkezi otoritelerin politik güçlerinin artırılması
4. Özel sektörle işbirliği, insan kaynağı geliştirilmesi, eğitim ve farkındalık gibi tamamlayıcı çalışmalar

ABD'de 2002 yılında oluşturulmuş merkezi koordinasyon kuruluşu DHS, belirli dönemlerde koordinasyon ve etki gücünü artırmış ve son olarak 2014 yılında en güçlü konuma gelmiştir. Almanya'da da benzer şekilde 2009 yılında kurulan BSI'ın yetkisi 2015 yılında belirgin seviyede artırılmıştır. ABD'de 2002, Almanya'da ise 2009 öncesi dönem, kurumların münferit çalışmalarının bir takım rehberlerle desteklendiği dönem olarak nitelendirilebilir. 2014-2017 dönemi ise siber güvenlik alanında ileri seviyedeki ülkelerde özel sektörle işbirliklerinin yoğun şekilde desteklendiği bir dönem olarak göze çarpmaktadır.

ABD'de bütçeden sorumlu Yönetim Bütçe Ofisinin siber güvenliğin kamu kurumları açısından en temel mevzuatı olan FISMA'nın uygulanmasından sorumlu tutulması, siber güvenlik politikalarında yürütülecek faaliyetlerin ekonomik güçle ne kadar iç içe olduğunun önemli bir göstergesi olarak görülmelidir.

ABD'de siber güvenlik alanındaki koordinasyonun Anayurt Bakanlığı tarafından yürütülmesi, ulusal güvenlikle siber güvenlik kavramlarının tamamen iç içe geçmiş kavramlar olduğunu göstermektedir. Siber güvenlik alanı, ülkeler açısından tamamıyla farklı dinamiklere sahip yeni bir savaş alanı hükmünde olup siber alanda yürütülen savaşlar ulusal boyut kazanmamış olmakla birlikte nicelik ve nitelik itibarıyla hızlı bir artış içerisindedir.

İncelenen ülkelerdeki siber güvenlik yapılanmasına bakıldığında, koordinasyon kuruluşlarının belirlenen eylemleri delege etmekten ziyade bizzat yakın işbirliği ile bu eylemleri yakından takip etmekte oldukları görülmektedir. Aşağıdaki bölümde değinileceği üzere, Bu yaklaşımın ülkemiz siber güvenlik politikalarındaki en temel eksikliklerden biri olduğu değerlendirilmektedir.

ABD'de siber güvenlik alanında Ar-Ge faaliyetleri yürüten DARPA kuruluşu, ülkemizdeki TÜBİTAK muhadili bir görev üstlenmektedir. Ancak DARPA'nın kuruluş olarak kendisini konumlandırdığı konum örnek alınabilecek niteliktedir. DARPA Ar-Ge faaliyetleri yürüteceği alanları stratejik bir bakış açısıyla tespit etmekte, belirli bir seviyede özel sektöre devri mümkün hale gelen Ar-Ge faaliyetlerinden çekilerek yeni alanlara yönelmektedir. Bu yaklaşımın ABD teknoloji sektöründeki olumlu yansımalarının oldukça bariz örnekleri bulunmaktadır.

İncelenen ülkelerde siber güvenliğin uluslararası boyutunun yakından takip edildiği, uluslararası kuruluşlarla oldukça yakın çalışıldığı görülmüştür. Gerek hukuki, gerekse teknik açıdan uluslararası işbirliklerinin oldukça önemli olduğu düşünülmektedir.

TÜRKİYE'DE MEVCUT DURUM VE ÖNERİLER

Çalışmanın bu kısmında Türkiye'nin siber güvenlik alanında halihazırda var olan kurum ve yapılar kısaca tanıtıldıktan sonra mevcut durumun geliştirilmesi ve iyileştirilmesi içi öneriler sunulacaktır.

Kurumsal Yapılanma

Türkiye'de kurumsal olarak siber güvenlikle ilgilenen birçok yapı olmasına rağmen, analizden de anlaşılacağı üzere temel sorulardan birisi korodinasyon ve uzman personel eksikliği göze çarpmaktadır. Bu bölümde, mevcut durumda aktif olan kurumlardan Siber Güvenlik Kurulu'ndan Bilgi ve İletişim Teknolojileri Kurumuna kadar bir dizi kurum kısaca tanıtılacaktır.

Kişisel Verileri Koruma Kurumu. Nisan 2016'da üst kurul olarak faaliyet gösterecek şekilde kurulan, idari ve mali özerkliğe sahip olan kurum, Başbakanlığa bağlıdır. Kurumun temel görevi Kişisel Verilerin Korunması Kanununun hükümlerinin etkin bir şekilde uygulanmasını sağlamaktır. Kurum bu kapsamda yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna ve Başbakanlığa sunmakla yükümlüdür. Kurum, idari yapısı itibarıyla Başkanlık ve bir Kuruldan oluşmaktadır. Kurul 9 üyeden oluşmakta olup beş üyesi Türkiye Büyük Millet Meclisi, iki üyesi Cumhurbaşkanı, iki üyesi Bakanlar Kurulu tarafından seçilir (Kişisel Verilerin Korunması Kanunu, 2016). Kurumun resmi internet sitesine bakıldığında Başkan, Başkan Yardımcısı ve 7 üyeden müteşekkil bir yapılanma oluşturulmuş olduğu görülmektedir (KVKK, 2017). Kurum tarafından ikincil mevzuat çalışmalarına başlanmıştır.

Siber Güvenlik Kurulu. 2012 yılında faaliyetlerine başlayan Siber Güvenlik Kurulunun görevi siber güvenlik alanında alınacak önlemleri belirlemek, hazırlanan strateji ve planları

onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak olarak belirlenmiştir. Kurulun ilk toplantısında 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı onaylanarak yürürlüğe girmiştir. Kasım 2016 itibarıyla Siber Güvenlik Kurulu 4 kez toplanmış olup son toplantı Şubat 2016'da gerçekleştirilmiştir. Süreç içerisinde değişen ihtiyaçlara uyum sağlamak amacıyla hazırlanan 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı da benzer şekilde Siber Güvenlik Kurulunca yürürlüğe girmiştir.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB). Ülkenin ulaşım ve haberleşme ağının koordinasyon, yönetim ve denetiminden sorumlu olan Bakanlığa, siber güvenlik alanındaki koordinasyon ihtiyacının artması sebebiyle 2012 yılında ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planlarını hazırlama ve koordinasyonunu sağlama görevi verilmiştir. Bakanlık ayrıca, aynı yıl hayata geçirilen Siber Güvenlik Kurulu tarafından onaylanan strateji ve planların hayata geçirilmesi sürecinin koordinasyonu ile görevlendirilmiştir.

Bilgi ve İletişim Teknolojileri Kurumu (BTK). Kurum temel olarak telekomünikasyon sektörünün düzenlenmesi ve denetiminden sorumlu olmakla birlikte bilişim, siber güvenlik ve telekomünikasyon arasındaki ilişkilerin karmaşıklaşmasıyla birlikte bu alanlarda da faaliyet göstermeye başlamıştır. BTK tarafından yürütülen faaliyetler arasında siber güvenlik tatbikatları önemli yer tutmaktadır. Nisan 2015 itibarıyla 3 ulusal ve 1 uluslararası siber tatbikat düzenlemiştir (BTK, 2015). Tatbikatlar teknik seviyede TÜBİTAK ile yakın işbirliği içerisinde yürütülmektedir.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK). Siber güvenlik alanındaki teknik çalışmalara TÜBİTAK öncülük etmektedir. 2010 yılında TÜBİTAK'ın bünyesinde kurulan Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM); bilgi güvenliği, kriptoloji ve haberleşme teknolojileri alanında hizmet vermektedir. Siber güvenlik faaliyetleri ağırlıklı olarak BİLGEM bünyesinde 2012 yılında kurulmuş olan Siber Güvenlik Enstitüsü (SGE) tarafından yürütülmektedir. BİLGEM altında faaliyet gösteren başka bir birim olan Ortak Kriterler Test Merkezi (OKTEM), uluslararası kabul görmüş bir ürün güvenliği standardı olan Ortak Kriterler (Common Criteria) standardına yönelik testler yapmaktadır. Ayrıca BİLGEM tarafından Siber Tehditleri Algılama Merkezi Sistemi (STAMPS), Siber Ortam Tuzak Sistemi (SORT), Veri Kaçağı Önleme Sistemi (VKÖS) ve benzeri bazı siber güvenlik çözümleri geliştirilmiştir (TÜBİTAK, 2016).

Türk Standardları Enstitüsü (TSE). 2013-2014 Siber Güvenlik Eylem Planı çalışmaları kapsamında TSE Bilişim Teknolojileri Test ve Belgelendirme Daire Başkanlığı bünyesinde 55 kadar bağımsız teknik uzmanın katılımıyla "Siber Güvenlik Özel Komitesi" kurulmuş ve bu kapsamda 20'den fazla güvenlik kriteri, standart ve rehber hazırlanmıştır.

Ulusal SOME Yapılanması. Siber Güvenlik Kurulu onayıyla UDHB koordinasyonunda hayata geçirilen stratejiler ve eylem planları çerçevesinde, BTK bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuş olup sektörel ve kurumsal çapta oluşturulacak Siber Olaylara Müdahale Merkezlerinin (SOME) faaliyetlerini bu ana çatı koordinasyonunda yürütmesi kararlaştırılmıştır (USOM, t.y.). Bu kapsamda ülkemizde 8'i sektörel, diğerleri kurumsal olmak üzere 515 adet SOME bulunmaktadır.

Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı. Siber suçlarla etkin mücadele edilebilmesi ve koordinasyonun sağlanması amacıyla 2011/2025 sayılı Bakanlar Kurulu Kararı ile Emniyet Genel Müdürlüğü bünyesinde kurulan Bilişim Suçlarıyla Mücadele Daire Başkanlığı, Şubat 2013 tarihli bir Bakanlık Oluru ile Siber Suçlarla Mücadele Daire Başkanlığı adını almıştır. Siber suçlarla mücadele il şube müdürlüklerinin kurulumu çalışmaları tamamlanmak üzeredir (EGM, t.y.).

KURUMSAL YAPILANMAYA İLİŞJKİN GENEL BİR DEĞERLENDİRME VE ÖNERİLER

Türkiye'de siber güvenliğe ilişkin 2013-2014 ve 2016-2019 yıllarını kapsayan iki adet strateji ve eylem planı hazırlanmış olup eylemlerin takibi UDHB koordinasyonunda yürütülmektedir. Her iki eylem planı da siber güvenliğin etki alanlarının tümünü kapsayacak nitelikte hazırlanmıştır. UDHB tarafından belirli dönemlerde eylemlere ilişkin raporlar alınarak paydaş çalıştayları düzenlenmektedir. Ancak siber güvenliğin gerektirdiği yakın işbirliği ve etkin veri paylaşımını sağlayacak teknik ve hukuki altyapıya ilişkin henüz ciddi bir ilerleme kat edilememiştir. Eylemlerde yaşanan sorunların çözümünde UDHB'nin bürokratik gücünün yetersizliği nedeniyle etkin önlemler alınamamakta, Siber Güvenlik Kurulunun müdahalesi gerekmektedir.

2012 yılında kurulmuş olan ve henüz dört kez toplanabilmiş olan Siber Güvenlik Kurulunun yapısına ve toplanma sıklığına bakıldığında, kimi zaman günlük stratejik kararlar alınmasını zorunlu kılan siber güvenlik alanı için bu tür bir yapılanmanın uygun olmadığı rahatlıkla söylenebilir. Siber güvenlik alanında yürütülecek çalışmalarda, paydaşlar arasında çıkabilecek muhtemel yetki karmaşalarının takip edilmesi, yeni teknolojilerin anlık olarak takip edilerek bunlardan kaynaklı yaklaşım farklarının yürürlükteki mevzuata vakitlice yansıtılması, gerekli ortak altyapı tesislerinde mevzuat kısıtlarının bulunması durumunda gerekli adımların hızlı ve etkin bir şekilde atılması gibi üst seviye gereksinimler söz konusudur. Bütün bu değerlendirme ve bilgiler, siber güvenlik alanında faaliyet gösteren merkezi bir otoritenin kurulmasının şart olduğuna işaret etmektedir. Kurulacak olan otorite kuruluş, Cumhurbaşkanlığı bünyesinde veya özerk nitelikli olabilir. Önemli olan husus, etki alanına giren konuda kurumlarla yakın işbirliğini engelleyecek seviyede bir bürokratik konuma sahip olmaması gerekliliğidir.

Teknik seviyede ulusal koordinasyon USOM çatısı altında SOME'ler aracılığıyla sağlanmakta, ancak kamu kurumları arası veri paylaşımına yönelik mevzuatın yetersiz olması sebebiyle SOME'ler ve USOM arasında etkin bilgi paylaşım ortamı oluşturulamamaktadır. Ayrıca kamu kurumlarınca yönetilen bilgi sistemlerine yönelik denetim mevcut durumda isteğe bağlı olup, zorunlu denetim imkânı da aynı sebeple mümkün olmamıştır.

Kamu kurumlarının siber güvenlik alanındaki faaliyetleri genellikle münferit projeler olarak yürütülmekte olup bir takım rehber ve yönlendirmeler mevcut olmakla birlikte ulusal ölçekte bir uygulama çerçevesi ve denetim mekanizması bulunmamaktadır. Kamu kurumlarında nitelikli bilişim personelinin istihdam edilebilmesini sağlayacak şartlar yeterince mevcut değildir. Kurumlarda güvenlik ürünlerinin temininde de bilgi ve birikim eksikliği bulunması sebebiyle, siber güvenlik ürün ve hizmetleri tedarik eden firmaların bilgi ve görüşleri ölçüsünde önlemler alınabilmekte, kurumlar çoğunlukla alternatif yöntem, araç ve çözümleri bilme ve test etme imkânına sahip olamamaktadır.

Kritik altyapı sektörlerinden olan enerji, bankacılık ve telekomünikasyon sektörlerinde, bu alanda yönlendirici otorite kuruluşların mevcut olmasının da etkisiyle siber güvenliğe ilişkin bir takım düzenlemeler hayata geçirilmiştir. Ancak kritik altyapı sektörlerinin birbirleriyle olan bağımlılık ilişkilerini de kapsayan bütüncül bir koruma yaklaşımı henüz geliştirilememiştir. Örneğin, elektrik şebekeleri pek çok e-devlet hizmeti ile diğer kritik altyapı sektörlerinin en temel girdisi durumundadır. Söz gelimi uzun süreli bir elektrik

kesintisinin bankacılık sektörüne olan etkisi henüz analiz edilerek gerekli önlemler alınmış değildir. Kritik altyapılarda yabancı ürün ve hizmetlere yüksek derecede bağımlılık söz konusudur. Alınan siber güvenlik önlemlerinin sistemlerin kritiklik seviyesi ile değil, kuruluş yetkililerinin konuya verdikleri önem derecesi ile orantılı olduğu gözlenmektedir. Ayrıca, kuruluşlar arası yoğun bilgi paylaşımı gerektiren bu alanda mevzuat kısıtları sebebiyle etkin bilgi paylaşımı yapılamadığı da bir gerçektir.

Dünya örneklerine bakıldığında, kamu bilgi sistemleri ve kritik altyapılar için tehdit oluşturan hususların takibinin bu alanda üst düzey kanuni güce sahip tek bir merkezden yapıldığı gözlenmektedir. Siber güvenlik tehditlerinin izlenmesi, analizi ve değerlendirmesi üst seviyede uzmanlık bilgisi gerektirdiğinden, bu görevin kamu kurumlarının her birinin münferit çabası ile yürütülmesinin beklenmesi doğru olmayacaktır. TÜBİTAK tarafından kamu kurumlarının talebi doğrultusunda kurulabilen balküpü sistemleri[13], bir yönüyle tehditlerin vakitlice algılanmasına ve bunlara yönelik önlemler geliştirilmesine destek olabilmektedir. Ancak bu sistemlerin çok sayıda kaynaktan alınacak zararlı yazılım ve siber saldırı verileriyle desteklenebileceği bir mekanizma oluşturulmadan bu sistemlerden herhangi bir verim alınabilmesi söz konusu değildir. Bu nedenle, bu sistemler tehditlerin bertaraf edilmesinde tek başına yeterli değildir. Bütüncül tehdit izleme sistemlerine ihtiyaç duyulmaktadır.

Yukarıda işaret edilen sorunlardan ve incelenen ülkelerden edinilen genel bilgilerden hareketle, siber güvenlik kurumsal yapılanmasında ele alınması önerilen temel bileşenler şunlardır:

1. Kamu bilgi sistemleri güvenliğinin sağlanması,
2. Kritik altyapıların güvenliğinin sağlanması,
3. Ulusal tehdit gözetleme sistemi kurulması.

[13] Balküpü sistemi, bilgi sistemlerine yetkisiz erişen saldırganlar ya da kullanıcılar hakkında bilgi toplamaya yarayan tuzak sunuculardır. Bu sistemler, istemli bir şekilde zafiyet barındırarak saldırganların bu zafiyetlerden faydalanmasını ve sistem üzerinde iz bırakmasını sağlar ve saldırgan asıl sisteme zarar verme aşamasına gelmeden önlem alınabilmesine imkân tanır.

Kurulacak merkezi otoritenin bu alanların her birinde ulusal koordinasyonu etkin şekilde sağlayacak bir yapıda olması gerekmektedir. Bu üç alan kendi içinde çeşitli bileşenlere ayrılmakla birlikte, birbirleri arasında da yoğun bir etkileşim söz konusudur. Bu nedenle, oluşturulacak ulusal politikalarda bütüncül bir yaklaşım ve alt kademede bu üç alanın her birinin kendi içinde detaylandırılması yerinde olacaktır.

Ulusal seviyede siber güvenlik önlemleri etkin bir veri paylaşım ortamını zorunlu kılmakta, mevcut durumda mevzuat kısıtları sebebiyle kurumlar arası etkin işbirliğinin sağlanamadığı gözlenmektedir. Mevzuat kısıtları hali hazırda sorumluluk sahibi kurumlara ilave sorumluluklar verilerek kısmen çözüme kavuşturulabilirse de, kurumlar arası hiyerarşiler dikkate alınarak oluşturulacak merkezi bir yapılanma, mevzuatın pratikte uygulanmasını büyük ölçüde kolaylaştıracaktır. Yapılanmada dikkate alınması gereken bir diğer önemli husus, oluşturulacak merkezi otoritenin asıl görevinin siber güvenlik alanında olması ihtiyacıdır. Siber güvenlik yapılanması kapsamında ele alınacak bileşenlerin her biri kendi içerisinde dallanmakta ve çok sayıda kuruluşun etkin koordinasyonunu gerektirmekte olup bu görevlerin kurumlara yüklenecek ilave görevler halinde ele alınması halinde siber güvenlik ile tam zamanlı ilgilenme ihtiyacı etkin bir şekilde karşılanamayacaktır.

REFERANSLAR

ACS (t.y.). Allianz für Cyber-Sicherheit - Über Uns. *Allianz für Cyber-Sicherheit (ACS)*. (çevrimiçi) https://www.allianz-fuer-cybersicherheit.de/ACS/DE/ Ueber_uns/ueber_uns. html (Almanca)

APCERT (t.y.). APCERT Official Homepage. *Asia Pacific Computer Emergency Response Team (APCERT)*. (çevrimiçi) http://www.apcert.org

BfDI (t.y.). BfDI Aufgaben. *Die Bundesbeauftrage für den Datenschutz und die Informationsfreiheit (BfDI)*. (çevrimiçi) http://www.bfdi.bund.de/DE/BfDI/ Artikel_BFDI/AufgabenBFDI.html

BITKOM (t.y.). BITKOM - About Us. *BITKOM Association*. (çevrimiçi) https://www.bitkom.org/EN/About-us/index-EN.html

BMI (2011). Cyber Security Strategy for Germany. *Bundesministerium des Innern (BMI)*. Berlin, Germany. Şubat 2011. (çevrimiçi) https://www.bsi.bund.de/SharedDocs/ Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf

BMI (t.y.). Federal Government Commissioner for Information Technology. *Bundesministerium des Innern (BMI)*. (çevrimiçi) http://www.bmi.bund.de/EN/Ministry/Commissioners/ information-technology/information-technology_node.html

BND (t.y). History of Bundesnachrichtendienst. *Bundesnachrichtendienst (BND)*. (çevrimiçi) http://www.bnd.bund.de/EN/About_us/History/History_node.html

BSA (2015a). EU Cybersecurity Dashboard – Country Reports – Japan. *The Software Alliance (BSA)*. Japan Section. Cybersecurity Country Reports. 2015. (çevrimiçi) http://cybersecurity.bsa.org/2015/apac/assets/PDFs/country_reports/cs_japan.pdf

BSA (2015b). EU Cybersecurity Dashboard – Country Reports – South Korea. *The Software Alliance (BSA)*. 2015. (çevrimiçi) http://cybersecurity.bsa.org/2015/apac/assets/ PDFs/country_reports/cs_southkorea.pdf

BSI (2009). Act to Strengthen the Security of Federal Information Technology. *Bundesamt für Sicherheit in der Informationstechnik (BSI)*. Kanunun Resmi İngilizce Çevirisi. 14

Ağustos 2009. (çevrimiçi) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf

BSI (t.y.). Commissoners - Federal Ministry of the Interior – English Information Webpage. *Bundesamt für Sicherheit in der Informationstechnik (BSI)*. (çevrimiçi) http://www.bmi.bund.de/EN/Ministry/Commissioners/commissioners_node.html

BTK (2015). Siber Güvenlik Tatbikatları. *Bilgi Teknolojileri ve İletişim Kurumu (BTK)*. (çevrimiçi) https://www.btk.gov.tr/tr-TR/Sayfalar/SG-Siber-Guvenlik-Tatbikatlari

Bundesnetzagentur (t.y.). The Bundesnetzagentur's Duties. (çevrimiçi) http://www.bundesnetzagentur.de/cln_1432/EN/General/Bundesnetzagentur/About/Functions/functions_node.html

BWE (t.y.). Initiative 'IT-Sicherheit in der Wirtschaft. *Bundesministerium für Wirtschaft und Energie (BWE)*. (çevrimiçi) http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/task-force.html

Byrne, Leo (2015). N. Korean Hacking Threat Leads to Blue House Cyber-security Office. *NK News Online Magazine*. 31 Mart 2015. (çevrimiçi) https://www.nknews.org/2015/03/n-korean-hacking-threat-leads-to-blue-house-cyber-security-office

CERT-Bund (t.y.). CERT-Bund - Das Computer-Notfallteam des BSI. *CERT-Bund*. Almanya. (çevrimiçi) https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/Cert-Bund/cert-bund_node.html

Daniel, Michael (2014). Assessing Cybersecurity Regulations. *White House Blog*. 22 Mayıs 2014. (çevrimiçi) http://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations

DARPA (t.y.). About DARPA. *Defense Advanced Research Projects Agency (DARPA)*. (çevrimiçi) http://www.darpa.mil/about-us/about-darpa

DHS (2016). National Infrastructure Coordinating Center. *U.S. Department of Homeland Security (DHS)*. (çevrimiçi) https://www.dhs.gov/national-infrastructure-coordinating-center

DNI (t.y.). Members of the Intelligence Community. *Office of the Director of National Intelligence (DNI)*. (çevrimiçi) https://www.dni.gov/index.php/intelligence-community/members-of-the-ic

EGM (t.y.). Emniyet Genel Müdürlüğü - Siber Suçlarla Mücadele Daire Başkanlığı. *Emniyet Genel Müdürlüğü (EGM)*. (çevrimiçi) https://www.egm.gov.tr/sayfalar/ sibersuclarlamucadeledairebaskanligi.aspx

Ferwerda, Jeremy; Choucri, Nazli; Madnick, Stuart (2010). Institutional Foundations for Cyber Security: Current Responses and New Challenges. Working Paper CISL#2009-03. Composite Information Systems Laboratory (CISL). Sloan School of Management. *Massachusetts Institute of Technology*. Cambridge. Eylül 2010.

Fischer, Erick A. (2012). Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions. Congressional Research Service. 7-5700. Rapor No:R42114. 29 Haziran 2012. (çevrimiçi) http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-073.pdf

FTC (2016). Privacy & Data Security Update (2015). Commission & Staff Reports. *Federal Trade Commission (FTC)*. Ocak 2016. (çevrimiçi) https://www.ftc.gov/reports/ privacy-data-security-update-2015

Horowitz, Michael (2016). Top Management and Performance Challenges Facing the Department of Justice – 2016. Memorandum for the Attorney General. FY 2016 Agency Financial Report. *Department of Justice*. 10 Kasım 2016.

Hunton & Williams LLP (2011). Germany Launches National Cyber Defense Center. Hunton & Williams Privacy and Information Security Law Blog. 7 Temmuz 2011. (çevrimiçi) https://www.huntonprivacyblog.com/2011/07/07/germany-launches-national-cyber-defense-center

IC3 (2008). 2008 Internet Crime Report. Internet Crime Complaint Center (IC3). (çevrimiçi) https://pdf.ic3.gov/2008_IC3Report.pdf

Internet-Beschwerdestelle.de (t.y.). About Us. Internet-Beschwerdestelle Initiative. (çevrimiçi) http://www.internet-beschwerdestelle.de/en/aboutus/index.htm

IPA (t.y.). About IPA. Japan Information-Technology Promotion Agency (IPA). (çevrimiçi) http://www.ipa.go.jp/english/about/about.html

Japan Cabinet (2000). Basic Act on the Formation of an Advanced Information and Telecommunications Network Society. Kanun No.144. Yayımlanma Yılı: 2000. Kanunun

Resmi İngilizce Çevirisi (çevrimiçi) http://www.cas.go.jp/jp/seisaku/hourei/data/BAFAITNS.pdf

JNSA (t.y.). Japan Network Security Association – About Us. Japan Network Security Association (JNSA). (çevrimiçi) http://www.jnsa.org/en/aboutus/index.html

JPCERT/CC (t.y.). JPCERT Coordination Center within APCERT. Japan Computer Emergency Response Team (JPCERT). Organizational Website. (çevrimiçi) https://www.jpcert.or.jp/english/apcert

KCC (t.y.). Korea Communication Commission – About the Organization – Establishment and Purpose. Korea Communication Commission (KCC). (çevrimiçi) http://eng.kcc.go.kr/user.do?page=E01010100&dc=E01010100

KCSC (t.y.). Korea Communications Standards Commission – About KCSC – Chairperson's Message. Korea Communications Standards Commission (KCSC). (çevrimiçi) http://www.kocsc.or.kr/eng/Message.php

KISA (t.y.). Korea Internet and Security Agency Official Website. Korea Internet and Security Agency (KISA). (çevrimiçi) http://www.kisa.or.kr/eng/main.jsp

Kişisel Verilerin Korunması Kanunu (2016). Kanun No: 6698 (24 Mart 2016). Resmi Gazete No: 29677 (7 Nisan 2016). (çevrimiçi) http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

KVKK (2017). Kişisel Verileri Koruma Kurulu Üyeleri. Kişisel Verileri Koruma Kurumu (KVKK) Resmi Web Sitesi. (çevrimiçi) http://www.kvkk.gov.tr/kuruluyeleri.html

MSIP (t.y.). About Ministry of Science, ICT and Future Planning – Organizational Structure. Ministry of Science, ICT and Future Planning (MSIP). (çevrimiçi) http://english.msip.go.kr/english/msipContents/contents.do?mId=Mjg1

Murray, Acklyn; Zeadally, Sherali; Flowers, Angelyn (2013). Cybersecurity and US Legislative Efforts to Address Cybercrime. *Journal of Homeland Security and Emergency Management*. ISSN (Online) 1547-7355. ISSN (Print) 2194-6361.

NICE (t.y.). About NICE. National Initiative for Cybersecurity Education (NICE). (çevrimiçi) http://csrc.nist.gov/nice/about/index.html

NIS (t.y). National Intelligence Service Korea – Major Duties – Cyber Security. National Intelligence Service Korea (NIS). (çevrimiçi) http://eng.nis.go.kr/EAF/1_7.do

NISC (2007). Japanese Government's Efforts to Address Information Security Issues – Focusing on the Cabinet Secretariat's Efforts. National Information Security Center (NISC). Kasım 2007. (çevrimiçi) http://www.nisc.go.jp/eng/pdf/overview_eng.pdf

NSA (2016). National Security Agency - Frequently Asked Questions. National Security Agency (NSA). 3 Mayıs 2016. (çevrimiçi) https://www.nsa.gov/about/faqs

PPC (2015). Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.. Korean Personal Information Protection Commission (PPC). 22 Aralık 2015. (çevrimiçi) http://www.pipc.go.kr/cmt/english/functions/communicationNetwork.do

PPC (t.y.a). Japan Personal Information Protection Commission – About The Commission – Roles and Responsibilities. Personal Information Protection Commission (PPC) Resmi Web Sitesi. (çevrimiçi) http://www.ppc.go.jp/en/aboutus/roles

PPC (t.y.b). Personal Information Protection Commission – Message from the Chairman. Personal Information Protection Commission (PIPC). (çevrimiçi) http://www.pipc.go.kr/cmt/english/introduction/chairman.do

Raul, Alan C.; Manoranjan, Tasha; Mohan, Vivek (2014). The Privacy, Data Protection and Cybersecurity Law Review. Editor: Alan Charles Raul. Law Business Research. Kasım 2014.

Thompson, Cadie (2015). These Images Show How Far Self-Driving Cars Have Come in a Few Short Years. Business Insider Online Magazine. 22 Ekim 2015. (çevrimiçi) http://www.businessinsider.com/the-first-self-driving-cars-that-competed-in-darpa-grand-challenge-2015-10

TÜBİTAK (2016). TÜBİTAK BİLGEM Teknoloji ve Çözüm Kataloğu. TÜBİTAK BİLGEM. s.125-129. (çevrimiçi) https://bilgem.tubitak.gov.tr/sites/images/bilgem_katalog_tr-2016.11.02.pdf

UP KRITIS (t.y.). About UP KRITIS Initiative. (çevrimiçi) http://www.kritis.bund.de/SubSites/Kritis/EN/activities/national/cipimplementationplan/cipimplementationplan_node.html

USOM (t.y.). Ulusal Siber Olaylara Müdahale Merkezi (USOM) Hakkında. Ulusal Siber Olaylara Müdahale Merkezi Resmi Web Sitesi. (çevrimiçi) https://www.usom.gov.tr/hakkimizda.html

U.S. Congress (2014). The Law Library of Congress - S.2521 - Federal Information Security Modernization Act of 2014. 113th Congress (2013-2014). 18 Aralık 2014. (çevrimiçi) https://www.congress.gov/bill/113th-congress/senate-bill/2521/text

U.S. Department of Justice (2013). U.S. Department of Justice FY 2014 Budget Request - Cyber Security - +$92.6 Million in Program Increases. U.S. Deparment of Justice. 2013. (çevrimiçi) http://www.justice.gov/jmd/2014factsheets/cyber-security.pdf

U.S. Department of Justice (2016). U.S. Department of Justice – Cybersecurity Unit. U.S. Department of Justice. About Computer Crime and Intellectual Property Section – Cybersecurity Unit. 21 Kasım 2016. (çevrimiçi) https://www.justice.gov/criminal-ccips/cybersecurity-unit

White House (2013). Presidential Policy Directive - Critical Infrastructure Security and Resilience. Office of the Press Secretary. White House. 12 Şubat 2013. (çevrimiçi) https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

White House (t.y.). National Security Council. National Security Council Homepage. White House. (çevrimiçi) https://www.whitehouse.gov/administration/eop/nsc