EDAM Siber Politika Kağıtları Serisi 2015/1

Türkiye'de Siber Güvenlik

Doç. Dr. Salih Bıçakcı

Öğretim Üyesi, Orta-Doğu ve Afrika Araştırma

ve Uygulama Merkezi Müdürü, Kadir Has Üniversitesi

Doruk Ergun

EDAM Araştırma Görevlisi

Prof. Dr. Mitat Çelikpala

Dekan, Sosyal Bilimler Yüksek Okulu,

Kadir Has Üniversitesi

25 Aralık 2015

Yönetici Özeti

- Türkiye'nin İnternet altyapısına yönelik 14 Aralık 2015'te başlayan dağıtık hizmet engelleme saldırısı (DDOS), siber saldırı kategorileri içinde temel ve etkili bir yöntemdir Bu tür saldırıların gerçek kaynağını tesbit etmek zordur. 24 Aralık 2015'de saldırıların artışıyla birlikte saldırıların Rusya kaynaklı olduğu yönünde tahminler yürütülmüştür. Hacker grubu Anonymous ise yaptığı bir açıklamayla saldırıyı üstlenmiştir. Buna göre Anonymous 25 Kasım 2015'de ilan ettiği #OpTurkey kampanyasını bir ay sonra en yüksek seviyeye taşımış olmaktadır. Sosyal medya kaynaklarında yapılan açıklamalardan Redhack grubunun da bu saldırılara katılmış olduğu görülmektedir.

- ODTÜ'nün yaptığı açıklamaya göre saldırının büyüklüğü (200+ Gbps) bu saldırının siber saldırı sıralamalarında önemli bir yere oturacağını söylemek mümkündür. İlk günlerde Ulusal Siber Olaylara Müdahale birimi USOM'un sessizliği ve kriz yönetiminin olmaması, kamu ve özel kurumların bu saldırıdan korunmaya yönelik karar almalarını zorlaştırmıştır. 24 Aralık 2015'te saldırı devlet kurumlarından bankacılık sektörüne doğru uzanmış ve birçok özel banka çalışamaz hale gelmiştir. Bu durum devlet ve özel kurumlar arasında stratejik iletişim yöntemlerinin çalışmadığının göstergesidir. Aktörlerin çokluğu saldırıların nasıl ilerleyeceğini tahmin etmemizi zorlaştırsa da yeni saldırıların Havayolları, Borsa gibi etkin ekonomi araçlarının ve yaygın belediye hizmetleri veren servisler olacağını muhtemeldir.

- Türkiye siber uzaydaki mevcudiyetini ve kabiliyetlerini özellikle 2010 senesinden sonra artan bir ivmeyle geliştirmiş olsa da, bu gelişme her alanda aynı seviyede olmamıştır; bunun neticesinde bazı alanlarda büyük aşamalar kaydedilse de diğer alanlarda beklenen ilerleme kaydedilememiştir. Başta Ulusal Bilgi Güvenliği Kanunu ve Kişisel Verilerin Korunması Mevzuatının çıkarılması olmak üzere, gerekli görülen adımların atılmasında yetersiz kalınmıştır. Bununla birlikte siyasi istikrarsızlıklar dolayısıyla ülkenin insan kaynağında da kayba uğradığı gözlenmektedir.

- Ülkenin siber güvenlik eylem planlarında ekseriyetle öne çıkarttığı hedefler; kritik altyapıların tanımlanması ve siber güvenliklerinin sağlanması, beşeri sermayenin geliştirilmesi, yerli yazılım ve donanımların geliştirilmesi, ulusal bir siber güvenlik stratejisinin oluşturulması ve yasal mevzuatın güçlendirilmesi olmuştur.

- Hâlihazırdaki kurumsal yapılanmada ülkenin siber güvenliğinin başlıca aktörleri Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın başını çektiği Siber Güvenlik Kurulu, kurulun kararıyla kurulmuş Ulusal Siber Olaylara Müdahale Merkezi (USOM), Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve bünyesindeki Telekomünikasyon İletişim Başkanlığıdır (TİB).

- Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ve plan doğrultusunda yapılan mevzuat uyarınca, Bankacılık ve Finans sektörünün de arasında yer aldığı kritik altyapı sektörlerinde, 7/24 esasına göre çalışan sektörel Siber Olaylara Müdahale Merkezi (SOME) kurulması zorunlu kılınmıştır. Mevcut şemaya göre kurumlar siber saldırıya uğradıkları durumda kendi kurumsal SOME'leri ve sektörel SOME'ler aracılığıyla olaylara müdahalede bulunacaktır, kendi kabiliyetlerini aşan durumlarda da USOM'un koordinasyonu ve desteğine müracaat edebileceklerdir.
- Türkiye'nin 2013-2014 eylem planındaki hedeflerinin bir kısmını hala gerçekleştirememiştir ve önümüzdeki dönemi kapsayan uzun vadeli bir siber güvenlik stratejisi ve eylem planı bulunmamaktadır.
- Türkiye, nüfusunun internet kullanma oranı konusunda dünyada geri sıralarda yer alsa da, dünya çapındaki siber saldırıların menşei olarak ilk 10'un içinde yer almaktadır.
- Türkiye'deki siber saldırganlar, niyet, ideoloji, kabiliyet ve eylem tarzları gibi konularda büyük farklılıklar göstermekte ve karmaşık bir tehdit ortamı oluşturmaktadırlar.
- Türkiye'deki hackerların çoğunlukla lise ve üstü eğitim kurumlarından mezun olmuş, 18-25 yaş arası, erkek, orta ve düşük gelir seviyeli ailelerden gelen bireylerden oluştuğu görülmektedir.
- Türkiye'nin siber güvenliğine tehdit oluşturmak açısından öne çıkan gruplar PKK Hack Team ve RedHack'tir. Siber uzayda yoğun faaliyet gösteren diğer grupların büyük çoğunluğunun devletçi olduğu, hatta bir kısmının devlet birimleriyle uyum içerisinde çalıştığı görülmüştür.

Giriş

Siber alanın doğuşu hem kullanıcılar hem de ulus devletlerin güvenlik kurumları için pek çok güvenlik riskini beraberinde getirmiştir. Siber alanı kullanarak saldırı düzenleyen kişiler, mali kurumları hedef alarak, ulusal sırlara erişip sızdırarak ve İran'ın nükleer tesislerini hedef alan Stuxnet solucanının da aralarında bulunduğu birçok örnekte görüldüğü gibi, ulusal altyapılara saldırıp kinetik bir saldırının gerçekleştirebileceği boyutta fiziksel hasarlar vererek, ciddi boyutta zarara yol açabilirler. Siber saldırıları kimin yaptığını belirlemek oldukça zordur, çünkü saldırganlar nadiren arkalarında iz bırakırlar ve hatta kendi konumlarını gizlemek için çabalarlar. Çoğu durumda siber saldırganların pahalı ya da nadir bulunan araçlara ihtiyacı olmaz. Hatta kamunun bilişim teknolojilerine erişiminin kolaylaşması ve bilişim teknolojilerinin hem kamu kurumlarının hem de özel kuruluşların işletilmesindeki rolünün git gide artması güvenlik zaaflarını daha da arttırmaktadır. Dağınık servis dışı bırakma (DDoS) saldırıları gibi birkaç istisna dışında, siber saldırılar, hedef sistemde ve siber güvenlik önlemlerinde var olan açıklardan yararlanarak yapılır[1]; müdafaa eden taraf bu açıkların ve dolayısıyla saldırının nereden gelebileceğinin farkında olmadığından siber saldırılara karşı savunma oldukça zordur. Ayrıca siber saldırganları öngörmek, silahsızlandırmak ve caydırmak daha zordur, bu da siber alanda taarruzun müdafaaya nazaran daha fazla avantajı olmasını sağlar.

Bu sıkıntılara rağmen, ulus devletler siber tehditlerle kendi kaynaklarıyla başa çıkmaya mecburdurlar. Dolayısıyla ulusların siber tehditlere ne kadar açık olduğunun ilk belirteci, ülkenin kendi kabiliyetleri ve siber güvenlik algısıdır. Bundan ötürü bu bölüm Türkiye'de siber güvenlik politikalarında ve mevzuatındaki gelişmelerin kronolojisini ve ülkenin siber güvenlik kabiliyetlerini inceleyerek başlamaktadır.

Bir ülkenin varlıklarına yöneltilen siber saldırılar, ülkenin kendi sınırları içinden doğmak zorunda değildirler. Ancak Türkiye ilginç bir vaka oluşturmaktadır, zira 2013 itibariyle Türkiye vatandaşlarının yalnızca yüzde 46'sının internet erişimi varken[2] (bu Türkiye'yi dünyada 97. sıraya koymaktadır), Türkiye dünyadaki siber saldırıların üçüncü büyük çıkış noktası olmuştur[3]. Bundan ötürü bu makalede ikinci olarak Türkiye'de halihazırda faal olan siber saldırganların, geçmişteki saldırıları, niyetleri ve mümkün olduğu durumlarda kabiliyetleri incelenecektir.

[1] Libicki, M. C. (2009) "Cyberdeterrence and Cyberwar" *Rand Corporation*
[2] International Telecommunications Union (Geneva) (2014) "Percentage of Individuals Using the Internet 2000-2013" 9 Kasım 2015 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls
[3] Bloomberg (2013, Nisan 23) "Top Ten Hacking Countries"

I. Türk Devletinin Kabiliyetleri ve Araçları

A) Bilgisayarla İşlenen Suçlar Üzerine Mevzuat

Mühim ulusal güvenlik meseleleri haline gelmeden önce, siber saldırılar ekseriyetle asayiş ve hukuku ilgilendiren meselelerdi. Dolayısıyla ordular sibere, kara, hava, deniz ve uzaydan sonra yeni bir savaş sahası olarak ilgi duymaya başlamadan önce, ulus devletler ilk olarak siber uzayın suç işlemek için kullanılmasına odaklanmıştır. Bu eğilim Türkiye'de de görülmüştür. Siber suçların Türk Ceza Kanunu'nda ilk yer alışı, 6 Haziran 1991 tarihli 3756 Sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun ile olmuştur. Bu değişikliğin 20. maddesi ile "Bilişim Alanında Suçlar" başlığı altında bir bab eklenmiş ve bir bilgisayardan programların, verilerin veya diğer unsurların hukuka aykırı olarak ele geçirilmesi veya bunların başkasına zarar vermek üzere kullanılması, nakledilmesi veya çoğaltılması yasayla ceza unsuru olarak kabul edilmiştir[4].

Siber suçların tanımı Eylül 2004 tarihinde 5237 sayılı Türk Ceza Kanunu ile genişletilmiştir. Ceza Kanunu tarafından üç adet bilişim suçu belirlenmiştir; bilişim sistemine girme başlıklı 243. madde, sistemi engelleme, bozma, verileri yok etme veya değiştirme başlıklı 244. madde (veri yerleştirme ve verilerin başka yere yönlendirilmesi de bu maddenin kapsamındadır) ve banka veya kredi kartlarının kötüye kullanılması üzerine 245. madde. [5] Bilgisayar veya telekomünikasyon cihazları gibi bilişim sistemlerinin kullanılması aracılığıyla (ancak bunlara münhasır olmadan) işlenebilecek diğer ilgili suçların arasında, özel hayatın gizliliği, haberleşmenin engellenmesi, hırsızlık, dolandırıcılık, kumar ve sahtecilik gibi birçok suç vardır. [6]

2000'lerin ikinci yarısında, Ankara, siber uzayın ülkenin milli güvenliğine zarar vermek için kullanılması ihtimaline daha çok ilgi göstermeye başlamıştır. 2006'da yapılan bir değişiklik ile siber suçlar 3713 sayılı Terörle Mücadele Kanunu'nda da yer almıştır. Değişiklikte şu ibare yer almaktadır: "Aşağıdaki suçlar 1 inci maddede belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde, terör suçu sayılır"[7] ve ardından Türk Ceza

---

[4] TBMM "3765 Sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun", Kanun No. 3756 Kabul Tarihi 6.6.1991 (Resmi Gazete ile yayımı: 14.6.1991, Sayı: 20901) 16 Temmuz 2014 tarihinde aşağıdaki adresten erişilmiştir: http://www.kanunum.com/files/kanun_tbmm_c074_03756.pdf ayrıca bakınız: http://www.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d18/c061/b127/tbmm180611270516.pdf

[5] Türk Ceza Kanunu (2004, Eylül 26) Kanun no: 5237

[6] Dokurer, S. (2002) "Ülkemizde Bilişim Suçları ve Mücadele Yöntemleri" EGM Bilgi İşlem Daire Başkanlığı Bilişim Suçları Büro Amirliği, 23 Eylül 2014 tarihinde aşağıdaki adresten erişilmiştir: http://bilisimsurasi.org.tr/dosyalar/17.doc

[7] 15 Temmuz 2003'te yapılan değişiklikler ile terörün tanımı üzerine olan birinci madde şu şekildedir: "Terör; cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve

Kanunu'nun birçok maddesi sıralanmaktadır. Sisteme izinsiz erişim, sistemin engellenmesi, verileri bozulması ve değiştirilmesi üzerine olan 243 ve 244'üncü maddelere ek olarak, bilişim sistemleri aracılığıyla işlenebilecek başka bazı suçlara da bu maddede yer verilmiştir[8]. Terörle Mücadele Kanunu'nun ikinci maddesine göre, kişiler bir terör örgütünün mensubu olmasalar bile, bir terör örgütü adına suç işlemeleri halinde terör suçlusu sayılır ve örgüt mensupları gibi cezalandırılırlar.

Bu esnada, kamu kurumları, Ankara'nın siber uzayda mevcudiyetinin ulusal güvenlik bakış açısının ötesinde, kamu hizmetlerinin sağlanması ve internet kullanımının düzenlenmesi gibi alanlarda nasıl olacağı konusunda aktif olarak politika üretmeye başlamıştır. 2011 senesinde yerini Kalkınma Bakanlığı almadan önce Devlet Planlama Teşkilatı konuyla ilgili bazı belgeler yayınlamıştır. Bunların arasında "e-Türkiye İnisiyatifi Eylem Planı 2002", e-Dönüşüm Türkiye Projesi ve Kısa Dönem Eylem Planı (2003-2004)" ve "e-Dönüşüm Türkiye Projesi 2005 Eylem Planı" vardır[9]. 2005 senesinde Devlet Planlama Teşkilatı "Bilişim Toplumu Stratejisi" isimli bir çalışma başlatmış ve 2006-2010 dönemini kapsayan bir strateji belgesi ve eylem planı yayınlamıştır; bu planların ana temalarından birisi ise güvenlik ve kişisel bilgilerin mahremiyeti olmuştur[10]. Eylem planı, siber güvenlik tehditlerini sürekli olarak takip etmesi, uyarılar yayınlaması, alınacak tedbirler konusunda bilgilendirme ve koordinasyon sağlaması amacıyla Bilgisayar Olaylarına Acil Müdahale Merkezi (SOME, *İngilizce CERT*) kurulacağını belirtmiştir. Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) altındaki Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nü (UEKAE) bu işin sorumlu kurumu olarak atamıştır[11]. 2006-2010 belgeleri bunun yanı sıra Kişisel Verilerin Korunması Kanun Tasarısı'nın 2006 sonuna kadar onanacağı ve ulusal güvenlik ile ilgili verilerin korunması ve devletin veri güvenliği sistemlerinin iyileştirilmesi için ek mevzuatların yürürlüğe konulacağını belirtmiştir.

Bu çabalara rağmen Meclis'e ilk olarak 2008 tarihinde sunulan Kişisel Verilerin Korunması Kanunu Tasarısı[12] hala onanmayı beklemektedir. Planlanan Bilgi Toplumu Genel Müdürlüğü'nu kuracak ve internet üzerinden e-Devlet portalından kamu hizmetlerinin sağlanmasını denetleyecek e-

---

dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir."

[8] Bunların arasında 113 sayılı kamu kurumu faaliyetlerinin engellenmesi, 142 sayılı nitelikli hırsızlık (bu maddenin 142.2.e bandında bilişim sistemlerinin kullanılmasına özellikle atıfta bulunulmaktadır), 151 ve 152 sayılı mala zarar verme ve mala zarar vermenin nitelikli halleri, 170 sayılı genel güvenliğin kasten tehlikeye sokulması, 213 sayılı halk arasında korku ve panik yaratmak amacıyla tehdit, ve belki de, **172 sayılı radyasyon yayma ve 173 sayılı atom enerjisi ile patlamaya sebebiyet verme** vardır.

[9] Şentürk, H. vd. (2012), "Cyber Security Analysis of Turkey" *International Journal of Information Security Science* Cilt.1, Sayı. 4

[10] T.C. Resmi Gazete, (2006, Temmuz 28) No: 26242, "Bilgi Toplumu Stratejisi Eylem Planı (2006-2010)". 16 Temmuz 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://www.resmigazete.gov.tr/eskiler/2006/07/20060728-7.htm

[11] A.g.e.

[12] T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü (2008, 22 April) "Kişisel Verilerin Korunması Kanunu Tasarısı" 18 Temmuz 2014 aşağıdaki bağlantıdan erişilmiştir: http://www2.tbmm.gov.tr/d23/1/1-0576.pdf

Devlet ve Bilgi Toplumu Kanun Tasarısı[13] da 2009 senesinin Ağustos ayından beri Meclis'te onanmayı beklemektedir.

Bununla birlikte 1990'ların sonunda ve 2000'lerin ilk yarısında, Milli Savunma Bakanlığı'nın koordinasyonluğunda, Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı adıyla bir başka kanun yazımı çalışmasında daha bulunulmuştur. Başbakanlık tarafından yapılan E-Türkiye İnisiyatifi Eylem Planı'na göre yasanın esasen 2003 ortasında tamamlanması ve onanması planlanmıştır[14]. Kanun taslağı Başbakanlık altında, ülkenin bilgi güvenliği politikalarını yönetmekle sorumlu ve Başbakan, Adalet, Milli Savunma, İçişleri, Dışişleri, Ulaştırma, Sanayi ve Ticaret Bakanları ile Milli Güvenlik Kurulu genel sekreteri, Genel Kurmay Muharebe Elektronik ve Bilgi Sistemleri Başkanı, Milli İstihbarat Teşkilatı (MİT) Müsteşarı ve TÜBİTAK'ın oluşturacağı bir Ulusal Bilgi Güvenliği Üst Kurulu'nun kurulmasını öngörmüştür[15]. Üst Kurul'un ayrıca tehditlerin değerlendirilmesi, ülkenin bilgi güvenliği politikalarının tayin edilmesi ve uygulanması ile ulusal bilgi güvenliği yönetmeliğinde yapılması önerilen değişikliklerin değerlendirilmesinden de sorumlu olması planlanmıştır.

Bu kanun aynı zamanda Ulusal Bilgi Güvenliği Kurumu Başkanlığının da kurulmasını tasarlamıştır. Başkanlığın beş ana hizmet biriminin olması düşünülmüştür, bunlar: Plan Program ve Koordinasyon, Bilgi Güvenliği, Kriptoloji, Bilgi Destek ile Denetleme ve Bilgilendirme Daire Başkanlıklarıdır. Her bir Daire Başkanlığı'nın, tehditlerin belirlenmesinden, ülkenin bilgi güvenliği mimarisinin oluşturulmasına, kripto sistemlerde kullanılabilecek yazılım ve donanımların tasdik edilmesinden, bilgi güvenliği araçlarının ithalat ve ihracat lisanslarının sağlanmasına kadar değişen birçok görevi olması düşünülmüştür. Kuruma, Uluslararası İlişkiler ve Hukuk Müşavirliği ile Ulusal Bilgisayar Güvenliği Merkezi Müdürlüğü destek sağlanması tasarlanmıştır. Ancak bu kanun daha sonra son taslak üzerinde uzlaşma sağlanamaması nedeniyle rafa kaldırılmıştır[16].

B) Türkiye'nin Siber Güvenlik Mimarisinin Kurumsallaştırılması

Bu gelişmelere paralel olarak, ülkede siber alandaki politikaların yürütülmesinden sorumlu kurumların kurulması adına adımlar atılmıştır. Bekleneceği üzere, konuya adanmış kurumların kurulması ülkenin siyaset üretme çabalarını hızlandırmış, internet üzerine mevzuatını zenginleştirmiş ve ülkenin kabiliyetlerini geliştirmiştir. Genel itibariyle bu kurumlar siber güvenliğin asayiş ve hukuki boyutuna odaklanmışlar ve siber savaş boyutunu Türk ordusuna bırakmışlardır. Bunun ana istisnasını

[13] T.C. Başbakanlık internet sayfasından 21 Temmuz 2014 terihinde aşağıdaki bağlantıdan erişilmiştir: http://www.basbakanlik.gov.tr/Handlers/FileHandler.ashx?FileId=1167
[14] T.C. Başbakanlık (2002, Ağustos) "e-Türkiye Girişimi Eylem Planı (TASLAK)"
[15] Aksakal, A. (1999) "Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı Taslağı" Türk Kütüphaneciliği Dergisi Cilt. 13 Sayı. 4 ss. 438-457
[16] Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı (2010, Mayıs) "Kritik Altyapıların Korunması"

araştırma kurumları oluşturmuştur; bu kurumlar Türkiye siber güvenlik mimarisinin her boyutunda, güvenilir yerli yazılım ve donanımların geliştirilmesinde çalışmaktadır ve dolayısıyla orduyla yakın bir ilişkileri olmaya devam etmektedir.

i. Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve Telekomünikasyon İletişim Başkanlığı (TİB)

2000 senesinin Ocak ayında kurulan Telekomünikasyon Kurumu, 2008 senesinin Kasım ayında Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) dönüştürülmüştür. BTK telekomünikasyon sektörünün düzenleyici kurumu olarak görev yapmaktadır ve yetkilendirme, denetleme, ihtilaf çözümü, tüketici haklarının korunması, sektör rekabetinin düzenlenmesi, teknik yönergeler yayınlamak ve spektrum yönetimi ve izlenmesinden sorumludur. Bunların yanı sıra kurum bilgi teknolojilerinden sorumlu otoritedir ve bu görevi Telekomünikasyon İletişim Başkanlığı (TİB) vasıtasıyla yerine getirmektedir. 2005 senesinde kurulan TİB doğrudan BTK Başkanı'na rapor vermekte ve olağan personelinin yanı sıra Milli İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı'nın ilgili birimlerinden birer temsilci barındırmaktadır.

TİB büyük oranda internetin de arasında bulunduğu telekomünikasyon araçları vasıtasıyla yapılan iletişimin ve sinyal bilgisinin takibi, gözetlenmesi, değerlendirilmesi ve kayıt edilmesiyle sorumludur. TİB aynı zamanda internet hizmetinin "emniyet" boyutuyla ilgili olarak içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcılarının denetlenmesiyle de ilgilenmektedir. Bundan ötürü TİB internete erişim özgürlüğü/internet sansürü ve kullanıcı mahremiyeti/ağ gözetlenmesi tartışmalarının tam ortasında yer alan ve tartışmaya yol açan bir kurum olmuştur. TİB bunların yanı sıra internet hizmetlerinin izlenmesi, perdelenmesi ve filtre edilmesi için yapılacak yazılım ve donanımlara ilişkin asgari kriterleri belirlemekle soruludur. Ulusal siber güvenlik mimarisinin bir parçası olan TİB, içerik, erişim ve yer sağlayıcıları ile diğer kurumların siber saldırıları tespit etmesi ve engellemesi için eşgüdüm de sağlamaktadır[17].

ii. TÜBİTAK

Türkiye'de elektronik ve kriptoloji araştırmaları yürüten sivil araştırma kurumlarının kökenleri Orta Doğu Teknik Üniversitesi'nde 1968 senesinde kurulan Elektronik Araştırma Ünitesi'ne dayanmaktadır. Başlangıçta beş kişiden oluşan birim, Marmara Bilimsel ve Endüstriyel Araştırma Enstitüsü'ne (daha sonra Marmara Araştırma Enstitüsü olarak adlandırılmıştır) bağlanmıştır ve

[17] Kanun No. 5651 Madde 10.6 (6 Şubat 2014 tarihinde yapılan düzenleme - 6518/95) Aşağıdaki adresten erişilebilir: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

ülkenin ilk milli kripto cihazı olan MİLON-1'i[18] Türk Silahlı Kuvvetleri'nın (TSK) ödüllendirdiği bir proje ile üretmiştir.

Ünite 1991 senesinde Elektronik ve Yarıiletken Teknolojileri Bölümü olarak adlandırılmış, 1995'te ise adı yine değişerek Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) halini almıştır. Bölüm Milli Savunma Bakanlığı ile Kriptoanaliz Test ve Dizayn Merkezi'nin kurulması için 1994 senesinde bir sözleşme imzalamış ve merkezi 1997 senesinde faaliyete geçirmiştir[19].

Aynı sene TÜBİTAK bünyesinde Ağ Güvenliği Grubu kurulmuştur. Grup Microsoft ve açık kaynak kodlu işletim sistemleri (OS), e-posta sunucuları, veritabanları ve bunların güvenlik açıkları ile sızma tespit edilmesi sistemleri üzerinde çalışmıştır. Bir sene sonra UEKAE doğrudan TÜBİTAK'a bağlanmıştır. TÜBİTAK'ın 2000 senesinde Milli Savunma Bakanlığı ile 2001 senesinde tamamlanacak Ortak Kriter Test Merkezi'nin kurulması için bir sözleşme imzalamıştır. Merkez daha sonra Ortak Kriter değerlendirme, haberleşme güvenliği (COMSEC), Yan Kanal Analizi (Side Channel Analysis) ve Tersine Mühendislik (Reverse Engineering) alanında yetkinlik kazanmıştır[20]. 2006 senesinde UEKAE, GÖKTÜRK uydu projesinin güvenliğini sağlama sorumluluğunu üstlenmiştir[21].

2006-2010 Eylem Planı uyarınca, TÜBİTAK 2007 senesinde dört kamu kurumuna Bilgi Güvenliği Yönetim Sistemini kurmuş ve farklı etkinliklerde kamu kurumları ve özel kuruluşlar için bilgi teknolojileri güvenliği günleri düzenlemeye başlamıştır. Yine 2007 senesinde TÜBİTAK UEKAE kendi ürünleri ile NATO tatbikatlarına katılmaya başlamıştır. Bunun yanı sıra bu dönemde TÜBİTAK UEKAE kurumsal SOME'ler arasında ortak SOME tatbikatları düzenlenmesini koordine etmeye başlamıştır. TÜBİTAK, Türkiye'de akreditasyona sahip iki SOME'den biri olan ve araştırma ve eğitim amacıyla işletilen ULAK-CSIRT'e ev sahipliği yapmaktadır[22]. Diğer SOME devlet tarafından işletilen TR-SOME'dir. 2007 senesinde ULAK-CSIRT NATO Bilgisayar Olaylarına Müdahale Yeteneği (NATO Computer Incident Response Capability – NCIRC) ile NCIRC ağına erişim, zararlı kod analizi, güvenlik açıkları veritabanı, uyarı/ikaz ve çalışan değişimi gibi konuları içeren bir anlaşma memorandumu imzalamıştır[23].

2010'da TÜBİTAK UEKAE ile (aslen Marmara Araştırma Merkezi altında yer alan) Bilişim Teknolojileri Enstitüsü (BTE), Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM)

---

[18] TÜBİTAK-BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü internet sayfası, "Tarihçe". 16 Temmuz 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://uekae.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce

[19] TÜBİTAK-BİLGEM internet sayfası, "Tarihçe". 16 Temmuz 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://bilgem.tubitak.gov.tr/en/kurumsal/history

[20] TÜBİTAK Siber Güvenlik Enstitüsü internet sayfası, "Tarihçe". 16 Temmuz 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://sge.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce

[21] TÜBİTAK-BİLGEM internet sayfası "History". 16 Temmuz 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://bilgem.tubitak.gov.tr/en/kurumsal/history

[22] Şentürk, H. vd. (2012), "Cyber Security Analysis of Turkey" *International Journal of Information Security Science* Cilt.1, Sayı. 4

[23] A.g.e.

adıyla birleştirilmiştir. Aynı sene Türkiye resmi olarak "Ortak Kriter" (ISO 15408) alanında "Sertifika Üreticisi" ülke olmuştur ve TÜBİTAK BİLGEM OKTEM (Ortak Kriter test merkezi) tarafından bilişim teknolojileri alanında sağlanan sertifikalar uluslararası geçerlilik kazanmıştır[24]. 2012 senesinde TÜBİTAK BİLGEM'de üç enstitü daha kurulmuştur, bunlar, Yazılım Teknolojileri Araştırma Enstitüsü (YTE), Siber Güvenlik Enstitüsü (SGE) ve İleri Teknoloji Araştırma Enstitüsüdür (İLTAREN). Ertesi sene TÜBİTAK BİLGEM NATO ile bir AR-GE (araştırma ve geliştirme) anlaşması, havacılık ve elektronik üzerine yoğunlaşan ve bir devlet şirketi olan HAVELSAN (Hava Elektronik Sanayi) ile de İşbirliği Mutabakatı imzalamıştır[25]. Yine 2013 senesinde BTE Türkiye'nin ilk Gerçek Zamanlı İşletim Sistemini (GİS) tasarlamış ve üretmiştir.

TÜBİTAK Ekim 2012'ye kadar siber güvenlikten sorumlu kurum olmuştur ve bu yetkisini 2012/3842 sayılı Bakanlar Kurulu Kararı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na devretmiştir[26]. TÜBİTAK şu anda milli kripto çözümlerinin yüzde 70'e yakınını sağlamaktadır[27]. TÜBİTAK, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDH) ve Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile birlikte, 81 ilde 164 farklı noktadan trafik toplayan ülkenin bal küpü (honey pot) siber tehdit tespit sistemini işletmektedir[28]. Görünürde sistemin bir parçası olan ama aslında tecrit edilmiş ve gözlem altında tutulan verilerin saldırganları açığa çıkartmak ve engellemek için yem olarak sunulduğu bal küpü sistemi, TİB'in yetkisi altında kurulmuştur.

Günümüze kadar Türkiye'de üç adet ulusal siber güvenlik tatbikatı olmuştur; biri 2008'de TR-BOME, diğerleri ise 2001 ve 2013'te TÜBİTAK ile BTK tarafından düzenlenmiştir. 2011 ulusal tatbikatı 41 tane kamu, özel ve devlet dışı kuruluştan 200'e yakın personelin katılımıyla gerçekleştirilmiştir. Katılımcılar arasında bilişim teknolojileri alanında çalışanların yanı sıra, finans, eğitim, sağlık, hukuk ve savunma sektörlerinden de katılımcılar olmuştur. 2013'te yapılan tatbikata 20'si gözlemci olmak üzere 61 tane kurum katılmıştır. Bu tatbikatta denenen senaryoların arasında log analizi, port taraması, DDoS, WEB güvenliği taraması, WEB uygulama testi, sosyal mühendislik ve bir "bayrağı ele geçir" yarışması olmuştur[29].

---

[24] TÜBİTAK-BİLGEM internet sayfası "History". 16 Temmuz 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://bilgem.tubitak.gov.tr/en/kurumsal/history

[25] A.g.e.

[26] Şentürk, H. vd. (2012), "Cyber Security Analysis of Turkey" *International Journal of Information Security Science* Cilt.1, Sayı. 4

[27] Bekdil, B. E. (2013, Aralık 1) "Cybersecurity an Emerging Market in Turkey" Defense News

[28] 30 Ocak 2015 tarihinde USOM ve TÜBİTAK tarafından Ankara'da yapılan Kurumsal SOME etkinliği sunumu, 14 Nisan 2015 tarihinde aşağıdaki bağlantıdan erişilmiştir: https://www.usom.gov.tr/faydali-dokuman/15.html

[29] Bilişim Dergisi "2. Ulusal Siber Güvenlik Tatbikatı Yapıldı" Sayı 151 ss:148-151 http://www.bilisimdergisi.org/s151/

iii. Müdahale Kabiliyeti Oluşturulması

Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından 2009 senesinin Mayıs ayında yayınlanan bir rapor[30], yukarıda değinilen taslak yasaların onanmasının yanı sıra, ülkenin siber güvenlik mevzuatını güçlendirmek için belli adımlar atması gerektiğini belirtmiştir. Bunların arasında; siber saldırıların nasıl inceleneceğine dair yönetmeliklere duyulan ihtiyaç, delillerin nasıl toplanacağının düzenlenmesi ve devletlerle bu konuya dair prosedürler ile güvenlik güçlerinin ve yargının siber alandaki yetkilerinin netleştirilmesi vardır. Raporda ayrıca hem güvenlik güçleri hem de yargıda teknik uzmanların yetersizliğine değinilmekte ve siber alandaki acil durumlara dair gerçekçi ve uygulanabilir planlara olan ihtiyacın altı çizilmektedir.

Bu sıkıntıların çoğu hala giderilmemiş olsa da geçtiğimiz birkaç sene içerisinde Ankara'nın siber güvenlik kabiliyetlerini arttırma çabaları ivme kazanmıştır. Örneğin Ulusal Güvenlik Siyaset Belgesi, diğer adıyla Kırmızı Kitap'a siber güvenlik başlığı Ekim 2010 ayında eklenmiştir[31]. Ertesi sene Emniyet Genel Müdürlüğü Bilişim Suçlarıyla Mücadele Daire Başkanlığı (Şubat 2013'te Siber Suçlarla Mücadele Daire Başkanlığı olarak yeniden adlandırılmıştır) kurulmuştur.

Haziran 2012'de düzenlenen Siber Güvenlik Strateji Çalıştayı'ndan sonra, Bilgi Güvenliği Derneği tarafından kaleme alınan bir tavsiye belgesi yayınlanmıştır. Belgede şu adımların atılması çağrısında bulunulmuştur[32]:

- *Ulusal Siber Güvenlik Strateji Belgesinin yayınlanması*
- *Ulusal Siber Güvenlik Kurulu oluşturulması*
- *Siber güvenlik alanında farkındalığın arttırılması ve siber güvenlik kültürünün yaygınlaştırılması*
- *Kişisel ve kurumsal verilerin korunması için daha sıkı tedbir alınması*
- *Uluslararası işbirliğinin güçlendirilmesi (belgede AB, ENISA, Avrupa Konseyi, BM, NATO ve AGİT sıralanmaktadır)*
- *Ulusal siber güvenlik Ar-Ge politikasının oluşturulması ve milli teknolojilerin geliştirilmesinin özendirilmesi*
- *Üniversitelerde konu üzerine yürütülen bilimsel çalışmaların arttırılması için adımlar atılması*
- *İnsan kaynaklarının yetiştirilmesi (bir diğer deyişle ulusal siber güvenlik uzmanlarının yetiştirilmesi)*
- *Kurumların ve güvenlik birimlerinin siber güvenlik kabiliyetlerinin geliştirilmesine yönelik adımlar atılması*
- *Kurumlara siber güvenlik sızma testleri yapacak bağımsız merkezlerin kurulması*
- *Yasal mevzuatın düzenlenmesi*

---

[30] Raporda Kurumun resmi görüşlerine yer verilmediğini belirten bir açıklama bulunmaktadır. Bkz. Unver, M. vd. (2009, Mayıs) "Siber Güvenliğin Sağlanması: Türkiye'de Mevcut Durum ve Alınması Gereken Tedbirler" Bilgi Teknolojileri ve İletişim Kurumu

[31] Sabah (2010, Ekim 28) "Kırmızı Kitap'a MGK'dan vize"

[32] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Bilgi Güvenliği Derneği (2012, Haziran) "Ulusal Siber Güvenlik Stratejisi: 2023'ün siber uzayında güçlü ve önder bir Türkiye için"

Belgede, aynı zamanda kritik altyapılardaki ve kamu ve özel kurumlardaki SOME'ler arasında koordinasyon sağlanması ve eğitim verilmesi için bir Türkiye Ulusal Siber Olaylara Müdahale Ekibinin (TC-SOME) kurulması gerektiği savunulmaktadır. Bununla birlikte merkezi bir ulusal siber tehdit ve korunmasızlık inceleme laboratuvarı kurulması ve bu laboratuvarda zararlı yazılımların incelenmesi ve yerli ve yabancı donanımların tasnifi ve derecelendirilmesinin yapılması önerilmektedir. Belgede ithal edilen donanımlarda bulunabilecek arka kapılara, yerleştirilmiş kötücül yazılımlara ve diğer güvenlik açıklarına değinilmekte ve ulusal donanım, ulusal bir işletim sistemi (OS), arama motoru ve internet tarayıcılarının geliştirilmesi çağrısında bulunmaktadır[33]. Ayrıca Savunma Sanayii Müsteşarlığı altında siber güvenlik alanında Ar-Ge yapmak ve koordinasyon sağlamak amacıyla bir Siber Güvenlik Mükemmeliyet Ağı kurulması önerilmektedir.

Bilgi Güvenliği Derneği'nin taslak belgesi ulusal kritik altyapı konusuna güçlü bir vurgu yapan ilk raporlardan[34] birisi olmuştur. Raporda kritik altyapılar şu şekilde tanımlanmıştır: "zarar görmesi veya yok olması toplumsal düzenin ve kamu hizmetlerinin devamlılığının sağlanmasında güçlük yaratacak; işlevlerini kısmen veya tamamen yerine getiremediğinde vatandaşların sağlığına, emniyetine, güvenliğine ve ekonomik faaliyetler veya hükümetin etkin ve verimli işleyişine olumsuz etki edecek yapıdır"[35]. Rapor aşağıda listelenen sektörlere ait yapıları kritik altyapı olarak değerlendirmektedir; bilişim, enerji, mali işler, sağlık, gıda, su, ulaşım, savunma, kamu güvenliği ve nükleer, biyolojik, kimyasal tesisler. Raporda aynı zamanda, kritik altyapıya sahip tüm kurumların her sene düzenlenen ulusal siber güvenlik tatbikatlarına katılmasının gerektiği ve 2013 sonuna kadar kritik altyapı işleten tüm kamu kurumu ve özel kuruluşlarının bünyesindeki bilişim teknolojisi altyapılarının 2013 sonuna kadar Bilgi Güvenliği Yönetim Sistemi standardına (TS ISO/IEC 27001) uyumlu hale gelmesinin gerektiği belirtilmektedir.

---

[33] Bu yönde bir teşebbüs Linux temelli bir işletim sistemi olan ve TÜBİTAK UEKAE tarafından geliştirilip, ilk olarak Aralık 2005'te yayınlanan Pardus projesi olmuştur. European Commission ISA Joinup (2008, Kasım 27) "A new kid on the block: The Turkish Pardus Linux Distribution"
Pardus kullanıcıları arasında Milli Savunma Bakanlığı (Pardus'e geçerek 2 milyon dolar tasarruf edildiği belirtilmektedir) ve Sosyal Güvenlik Kurumu vardır. NTVMSNBC (2009, Nisan 14) "MSB, Pardus ile 2 milyon dolar tasarruf etti" NTVMSNBC (2009, Nisan 13) "SGK, Pardus'a göç etmeye hazırlanıyor".
Proje 2011'de, iddia edildiğine göre TÜBİTAK'taki siyasi değişimler sonucunda işgücünde büyük kayıplar olması sebebiyle, durmuştur. www.shiftdelete.net (2012, Şubat 01) "Yerli Pardus'ta Sona Doğru" 9 Eylül 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://shiftdelete.net/yerli-pardusta-sona-dogru-34654?p=1
2 sene boyunca hiç yeni sürüm yayınlanmamasından sonra işletim sisteminin 2013 sürümü yayınlanmıştır. Ağustos 2014'te hükümetinin programından bahseden Başbakan Ahmet Davutoğlu Pardus projesine açıkça değinmiş ve hükümetin amacının Pardus'ü kamu kurumları ve özel kuruluşlara yaymak olduğunu belirtmiştir. Pardus Portal internet sayfası (2014, Ağustos) "PARDUS 62. Hükümet Programında Yerini Aldı!" 9 Eylül 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://www.pardus.org.tr/pardus-hukumet-programinda

[34] BTK çalışanları tarafından Mayıs 2010'da kaleme alınan daha eski bir raporda kritik ulusal altyapı (KUA) konusunda uluslararası tanımlamalar ve mevzuat incelenmiş ve Türkiye'de KUA konusunda atılan adımların noksanlığına dikkat çekilmiştir. Bkz. Ünver, M. vd. (2010, Mayıs) "Kritik Altyapıların Korunması" Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı

[35] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Bilgi Güvenliği Derneği (2012, Haziran) "Ulusal Siber Güvenlik Stratejisi: 2023'ün siber uzayında güçlü ve önder bir Türkiye için" ss.11-12

iv. Siber Güvenlik Kurulu

Raporun çizdiği rotada atılan ilk adım 20 Ekim 2012 tarihinde 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin" Bakanlar Kurulu Kararı ile atılmıştır. Bu karar "siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla"[36] Siber Güvenlik Kurulu'nu kurmuştur. Ulaştırma, Denizcilik ve Haberleşme (UDH) Bakanı'nın başkanlığını yaptığı Kurul, Dışişleri, İçişleri, Milli Savunma, UDH Bakanlıkları müsteşarlarının yanı sıra, Kamu Düzeni ve Güvenliği Müsteşarı, MİT Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, BTK Başkanı, TÜBİTAK Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ve UDH tarafından belirlenen bakanlık ve kamu kurumu üst düzey yöneticilerinden oluşmaktadır.

2012/3842 sayılı Bakanlar Kurulu Kararı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na aşağıdaki görevler verilmiştir[37]:

- *Ulusal Siber Güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak*
- *Kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenliği ile mahremiyetinin güvence altına alınmasını sağlamaya yönelik usul ve esasları hazırlamak*
- *Ulusal Siber Güvenliğin sağlanmasında kamu kurum ve kuruluşlarında teknik altyapının oluşturulmasını takip etmek, uygulamaların etkinliğinin doğrulanmasını ve test edilmesini sağlamak*
- *Ulusal bilgi teknolojileri ve iletişim altyapısı ve sistemleri ile veri tabanlarının güvenliğini sağlamaya, kritik alt yapıları belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri kurmaya, kurdurmaya, bu sistemlerin denetimi, işletimi ve sürekli güçlendirilmesine yönelik çalışmalar yapmak*
- *Ulusal Siber Güvenliğin sağlanmasında her türlü milli çözümlerin ve siber saldırılara müdahale araçlarının geliştirilmesi ve üretilmesini teşvik etmek, kullanımını sağlamak*
- *Ulusal Siber Güvenlik açısından kritik kurum ve konumlar için gerekli ve yeterli sayıda uzman personelin temini, eğitimi ve gelişimini planlamak, koordine etmek ve yürütmek*
- *Bu Karar çerçevesinde diğer ülkeler ve uluslararası kuruluşlarla işbirliği yapmak*
- *Ulusal Siber Güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek*
- *Bilgi güvenliği alanında eğitim, test ve çözüm üretme alanında çalışan gerçek ve tüzel kişilere usul ve esaslarını belirleyerek güvenlik belgesi vermek*
- *Siber Güvenlik Kurulunun sekretarya hizmetini yürütmek*

[36] Bakanlar Kurulu Kararı 2012/3842 20 Ekim 2012 tarihli 28447 sayılı Resmi Gazete'de yayınlanmıştır.
[37] Bakanlar Kurulu Kararı 2012/3842 #5.1 20 Ekim 2012 tarihli 28447 sayılı Resmi Gazete'de yayınlanmıştır.

Ertesi sene Siber Güvenlik Kurulu ülkenin ilk Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nı[38] yayınlamıştır ve plan 2013/4890 sayılı 25 Mart 2013 tarihli Bakanlar Kurulu Kararı ile yürürlüğe girmiştir. Eylem planında *kritik altyapılar* şu şekilde tanımlanmaktadır:

"İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda,

- *Can kaybına,*
- *Büyük ölçekli ekonomik zarara,*
- *Ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına,*

yol açabilecek bilişim sistemlerini barındıran altyapılar"[39].

Eylem planında çoğu kritik hizmet ve altyapının internet bağlantısı olması ve faaliyetlerini sürdürmek için bilişim sistemlerine bağlı olmalarından ötürü kritik altyapıların siber tehditlere açık olduklarını belirtmektedir. Ayrıca Türkiye'deki güvenlik zaaflarının, siber uzayın tabiatında bulunan sistemle ilgili güvenlik açıklarının yanı sıra, toplum genelinde, kurumlarda ve yüksek düzeyli yöneticiler arasında siber güvenlik hakkındaki bilgisizlikten kaynaklandığına dikkat çekilmektedir. Eylem planı bunların yanı sıra, bilişim sistemleri altyapısı, uzmanları ve koordinasyon eksikliğine ve ulusal ve uluslararası mevzuatın yetersizliğine değinmektedir.

2013-2014 eylem planı, 2012'de gerçekleştirilen çalıştayın tavsiye raporunun üstüne ilave tavsiyeler eklemiş ve toplamda 29 adet eylemin gerçekleştirilmesi için planlama yapmıştır. Bu iddialı eylem planları pek çok paydaşı kapsamaktadır; bunların arasında bakanlıklar, araştırma kurumları, özel sektör ve ülkenin siber güvenliğini korumakla görevli kurumlar bulunmaktadır. Kritik altyapılar eylem planında ekseriyetle vurgulanmıştır. 5 numaralı eylem, kritik altyapılarda yürütülecek bilgi güvenliği programına değinmektedir ve siber saldırıların doğrudan hedefi olabilecek kritik altyapıları belirleme ve belirlenecek bir kritik altyapının sektörel risk analizinin yapılması görevlerini TÜBİTAK'a vermektedir. Ayrıca kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar, sektörel risk analizi yöntemlerinin ve sektörel acil eylem planlarının gereksinimlerinin belirlenmesi, yıllık risk analizi raporlama çalışmalarının yapılması ile sektörel iş sürekliliği planlarının gereksinimlerinin ve sektörel güvenlik önlemlerinin belirlenmesi ve uygulanmasından mesul olmuştur[40]. Bununla birlikte 10 numaralı yazılım güvenliği programının yürütülmesi eylemi ile TÜBİTAK, kritik altyapılarda kullanılmak üzere geliştirilen yazılımlar için güvenlik yazılım geliştirme temel kuralları dokümanının yayımlanması ve "kritik altyapılar için geliştirilen yazılımların güvenlik değerlendirmeleri kapsamında

[38] Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve İletişim Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"
[39] Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve İletişim Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" s.3
[40] Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve İletişim Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" s.15

ilgili kurumların bünyesinde gerekli teknik isterlerin uygulanması ve kontrolüne yönelik fizibilitenin hazırlanarak Siber Güvenik Kuruluna sunulmasından"[41] sorumlu tutulmuştur.

Kritik altyapıyı güçlendirmenin yanı sıra, bazı eylem maddeleri, vakaların olası etkilerinin en aza indirilmesi ve dirençliliğin geliştirilmesi üzerinedir. 16 numaralı eylem ile UDH veri sızmasını tespite yönelik test altyapısı geliştirilmesi ve uygulamaya alınmasından ve 14 numaralı eylem ile iş sürekliliği ve veri yedekleme sistemleri kurulmasından sorumlu tutulmuştur. Ayrıca TÜBİTAK ve Türk Standardları Enstitüsü ile siber güvenlik alanındaki ürünlerin ve hizmet sağlayıcıların sertifikalandırılmasından sorumludur.

Eylem planının en büyük önceliklerinden biri ülkenin beşeri sermayesinin geliştirilmesidir. En az 9 adet eylem siber güvenlik alanında bilgilendirme ve yetkinlik kazandırılması üzerinedir. Örneğin, bu eylem maddeleri, farkındalığın artırılması, bilişim sistemleri uzmanları yetiştirilmesi, siber güvenlik tatbikatları ve etkinlikleri düzenlenmesi, konu üzerine verilen derslerin ve bölümlerin artırılması gibi eylemleri içermektedir. Bununla birlikte 11 numaralı eylemle BTK'ya siber tehditlerin tespit edilmesi, izlenmesi ve önlenmesi için mekanizmalar geliştirmesi görevi verilmiştir; buna tehditlerin tespit edilmesi amacıyla bir bal küpü sisteminin geliştirilmesi de dahildir.

Bir diğer vurgu, üniversitelerde Ar-Ge laboratuarları kurulması, proje teşviği sistemlerinde siber güvenliğin öncelikli konular arasına eklenmesi, kamu kurumları, özel kuruluşlar, devlet dışı kurumlar, üniversiteler ve bilişim uzmanları ile siber güvenlik alanında milli ürünler ve çözümler yaratılması için düzenli faaliyetlerde bulunulması gibi yöntemlerle siber güvenlik alanında milli teknolojilerin geliştirilmesi üzerinedir. Strateji belgesinde aynı zamanda ulusal mevzuattaki yetersizliğe değinilmekte ve Adalet Bakanlığı ve ilgili bakanlıklara ihtiyaç duyulan düzenlemelerin belirlenmesi için çağrıda bulunulmaktadır. Ayrıca Türk Dil Kurumu'na siber güvenlik terimler sözlüğü yaratma görevi verilmiştir.

v. Ulusal Siber Olaylara Müdahale Merkezi (USOM)

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın bir getirisi de tehditlerin farkedilmesi ve uyarıların geliştirilip paylaşılması amacıyla kurulan bir Siber Olaylara Müdahale Merkezi kurulması olmuştur. Strateji belgesi, TİB'in denetimi altında "ülkemizi etkileyebilecek tehditlere karşı 7/24 müdahale esasına göre çalışacak "Ulusal Siber Olaylara Müdahale Merkezi[nin] (USOM)" ve USOM'un koordinasyonunda çalışacak sektörel "Siber Olaylara Müdahale Ekipleri[nin]

[41] Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve İletişim Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" s.18

(SOME)"[42] kurulması çağrısını yapmıştır. USOM ayrıca kritik altyapı sektörleri ve kamu kurumları için sektörel SOME'ler kurmakla ve bunlara eğitim ve koordinasyon sağlamakla görevlidir.

11 Kasım 2013 tarihinde, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliği yayınlamıştır[43]. Tebliğe göre bakanlıklar kendi kurumsal SOME'lerini ihtiyaç doğrultusunda, alt birimlerini ve ilgili kurumları kapsayacak şekilde kurmalıdırlar. Diğer tüm kamu kurumları, alt kuruluşlar, bakanlıkların ilgili birimleri ile özel kurum ve kuruluşlar kendi kurumsal SOME'lerini kurabilirler. Hedef kritik altyapı işleten firmalara ve kendi bilişim teknolojileri birimleri olan bütün bakanlıklara ve diğer kamu kurumlarına birer kurumsal SOME kurmaktır. Ocak 2015 itibariyle 720 personelle işletilen 245 kurumsal SOME kurulmuştur[44]. Kurumsal SOME'lerin kurulmasını koordine etme görevi UDH'ye verilmiştir.

Siber Güvenlik Kurumu tarafından belirlenecek kritik sektörlerin sektörel SOME'leri olması mecbur kılınmıştır. Düzenleyici ve denetleyici kurumların sektörel SOME'leri BTK tarafından koordine edilmektedir. Şu ana kadar 6 adet kritik sektör belirlenmiştir; bunlar, bankacılık ve finans, ulaştırma, enerji, kritik kamu hizmetleri, su yönetimi ve elektronik haberleşmedir[45]. Kritik altyapı işleten kamu ve özel kuruluşların sektörel SOME'ler altında çalışacak kurumsal SOME'ler açma yükümlülüğü vardır.

Bütün SOME'lerin 7/24 esasıyla çalışması ve kanun dışı olabilecek her faaliyeti yargı birimlerine ve USOM'a anında haber vermesi gerekmektedir. SOME'ler, siber saldırılara karşı gerekli tedbirleri almak, müdahale ve olay kayıt sistemleri kurmak ve kurumlarının bilgi güvenliğini sağlamakla yükümlüdürler. Eğer bir olay müdahale yeteneklerinin ötesindeyse sektörel SOME'lere ve/veya USOM'a yardım için başvurabilirler. Ayrıca USOM, SOME'lere eğitim vermekle yükümlüdür ve gerekli görmesi halinde kurumsal ve sektörel SOME'lerle doğrudan çalışabilir. Uluslararası kurumlarla veya uluslararası denk birimlerle işbirliği USOM tarafından yürütülür. Halihazırdaki kurumsal yapısına göre USOM şu konularla ilgilenen 5 birimden oluşmaktadır; siber olay raporlaması ve iletişim, zararlı yazılım analizi, kurumlar arası işbirliği, yazılım geliştirilmesi ve uluslararası iletişim[46]. Kurum 2014 başı ile 2015 senesinin Ocak ayı arasında kamu kurumlarını ve özel sektörü hedef alan 1500'den fazla olay tespit etmiştir.

---

[42] Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve İletişim Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" s.8

[43] Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, 11 Kasım 2013 tarihli 28818 sayılı Resmi Gazete'de yayınlanmıştır

[44] USOM ve TÜBİTAK tarafından 30 Ocak 2015 tarihinde Ankara'da düzenlenen Kurumsal SOME Etkinliği sunumu. 14 Nisan 2015 tarihinde aşağıdaki bağlantıdan erişilmiştir: https://www.usom.gov.tr/faydali-dokuman/15.html

[45] BTK internet sayfası "USOM-SOME" 14 Nisan 2015 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/usomsome.php

[46] A.g.e

Birçok açıdan bakıldığında, USOM Türkiye'deki kritik altyapının korunmanın asli kurumu ve siber güvenlik krizlerinin yönetimi için iyi bir aday konumundadır. Ancak USOM, diğer kamu kurum ve kuruluşlarına yönlendirmek için gerekli koordinasyon yetkisiyle donatılmamış durumdadır. Oysa ülke çapında gelişebilecek siber güvenlik krizlerinin çoğunluğunun yönetimi kapsamlı bir iletişim, işbirliği, koordinasyon ve yeni politika uygulamalarını gerekli kılmaktadır. Ulusal SOME'nin de böyle bir görevi yerine getirebilmek üzere tasarlanmadığı görülmektedir.

Diğer yandan, enerji dağıtımı, su işleme, ulaştırma, kimyasal, yönetim, savunma ve gıda süreçlerini de içeren kritik altyapının çoğunluğu endüstriyel süreçlerin önemli bir parçası olan endüstriyel kontrol sistemleri (SCADA dâhil) üzerinde çalışmaktadır. Bu Endüstriyel Kontrol Sistemlerini güvenlik altına almak, içinde sektörel farklılıkları görebilmeyi de gerektiren özel bir uzmanlığı zorunlu kılmaktadır. Bu türdeki bir özel uzmanlık talebi pek çok devleti Endüstriyel Kontrol Sistemleri Bilgisayar Acil Durum Müdahale Timleri (EKS–SOME) kurmaya zorlamaktadır. Türkiye, kritik altyapı korumasına odaklanabilecek bir EKS–SOME'ye sahip değildir.

vi. Afet ve Acil Durum Yönetim Başkanlığı (AFAD)

Öte yandan Türkiye'de Siber Kriz Yönetimi ve Kritik Altyapı Koruması görevi 5902 sayılı kanunla Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı'na (AFAD) verilmiştir. Kanunda AFAD'ın görevi afetlerle, hem afet esnasında hem de sonrasında mücadele eden kurum ve kuruluşlar arasında koordinasyonunu sağlamak ve bunu düzenleyecek politikaları geliştirmek şeklinde tanımlanmaktadır. AFAD bu çerçevede bir eylem planı hazırlayarak afetleri başlıca iki gruba ayırmıştır: doğal afetler ve teknolojik afetler. Kritik Altyapı Koruma ve siber güvenlik konuları, bu bağlamda teknolojik afetler kategorisinde yer almaktadır. AFAD, Kritik Altyapı Koruma Planı çerçevesinde aralarında çeşitli bakanlıkların da bulunduğu 12 kurum ve kuruluşu bu sürecin anahtar üyeleri olarak belirlemiştir. Bunlar: İçişleri, Çevre ve Şehircilik, Enerji ve Tabi Kaynaklar, Sağlık, Ulaştırma, Denizcilik ve Haberleşme ile Bilim, Sanayi ve Teknoloji bakanlıkları ve Enerji Piyasası Düzenleme Kurumu, Türkiye Atom Enerjisi Kurumu, TÜBİTAK, Jandarma Genel Komutanlığı, Kamu Düzeni ve Güvenliği Müsteşarlığı ve Hacettepe Üniversitesi'dir. AFAD, koruma sürecinin temel aşamalarını tanımlamak için Eylül 2014'te 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi'ni yayınlamıştır. Belgede gereksinimler ve bunların gerçekleştirilmesi için öngörülen eylemler belirlenmiştir. Tanımlanan gereksinimler şunlardır:

- Yetkili (sorumlu) Otoritelerin Belirlenmesi.
- Yetkili koordinasyon otoritesinin belirlenmesi, iş bölümü bazında kritik altyapı sektörleri (KAS) belirlemekte kullanılacak kıstasların tespit edilmesi.

- Avrupa Birliği Direktifinin uyumlaştırılması ile ilgili taslak yönetmelik hazırlanması ve kapsam, büyüklük ve zaman etkisi faktörlerinin göz önünde bulundurularak kritik altyapılarının belirlenmesi ve koruyucu tedbirlerin arttırılması.
- Kritik altyapıların etkin korunması, ulusal seviyede veya AB seviyesinde bütün ilgili paydaşlar arasında iletişim, koordinasyon ve işbirliği.
- KAS'lerle ilgili işletmeci güvenlik planı yapılması.
- Güvenlik İrtibat Görevlisi atamak.
- Eğitim programı oluşturulması ve uygulanması.
- Ulusal düzeydeki kritik altyapıların korunması amacı ile Kritik Altyapı Koruma Planı hazırlanması.
- En iyi uygulamaların ve anlık tehdit ve alarmların güvenli bir şekilde paylaşımı yoluyla uygun koruma tedbirlerinin geliştirilmesini teşvik edebilecek AB Kritik Altyapı Uyarı Bilgi Ağı (KAUBA) çalışmalarına entegrasyon.
- Raporlama.

Yol Haritası Belgesi'nde, yerine getirilmesi planlanan görevler için 2016 en yakın, 2018 ise en uzak tarihler olarak belirlenmiştir. Yol Haritası AFAD'ın herhangi bir siber güvenlik krizini nasıl yöneteceğine açıklık getirilmemektedir.

C) Silahlı Kuvvetlerin Siber Güvenlik Mekanizmaları

Türkiye'de kamu kurum ve kuruluşları ile özel sektör unsurlarına yönelik olarak özellikle Estonya ve sonrasında Gürcistan'a karşı gerçekleştirilen siber saldırı fırtınası sonrasında, artan siber saldırılar idareyi siber saldırıları bir tehdit olarak tanımlama yönünde adım atmaya zorlamış ve süreç sonunda da ulusal siber güvenlik stratejisini inşa etmenin yolunu açmıştır. Milli Güvenlik Kurulu da siber güvenliği bir tehdit olarak tanımlayarak tehdidi "Kırmızı Kitap" olarak adlandırılan askeri strateji belgesine ekledi. Bu sırada, farklı bir gelişme daha yaşandı ve NATO 17 Mayıs 2010'da siber güvenliği üye ülkelere yönelik bir tehdit olarak tanımlayan yeni strateji belgesini açıkladı.

Türkiye'nin siber ordusu olarak bilinen Siber Savunma Komutanlığı'nın oluşturulması kararı da bu dönem denk gelmektedir. Ülkeye yönelik siber saldırılara karşı savunmayı amaçlayan Komutanlık Savunma Bakanlığı, TÜBİTAK ve Orta Doğu Teknik Üniversitesi işbirliğinde Genel Kurmay Başkanlığı bünyesinde görev yapacak özel bir birimi şeklinde planlanmıştır.

Takip eden dönemde, Siber Güvenlik Kurulu'nun kurulmasıyla birlikte Türk Silahlı Kuvvetleri (TSK) de Haziran 2012'de Siber Güvenlik Merkez Başkanlığını kurmaya karar vermiştir. Bu yapılanma, bir siber komutanlık olmaktan çok uzak olmakla birlikte TSK'ya destek olan bir SOME merkezi niteliğinde olması nedeniyle iyi bir başlangıç olarak kabul edilebilir. TSK 2013'te, Ulusal Siber Güvenlik Stratejisinin ilanını takiben de Siber Savunma Komutanlığı'nın kuruluşunu ilan etmiş ve görevlerini şöyle tanımladı;

1. TSK'nın kullandığı siber ortamda bulunan tüm sistemlerin siber savunması sağlamak.
2. Siber olaylara 7/24 esasına göre müdahale etmek
3. Ulusal olarak ve NATO tarafından icra edilen tatbikatlara iştirak etmek.
4. TSK çapında bilinçlendirme ve eğitim faaliyetleri yürütmek.
5. TSK tarafından kullanılan ağlarda düzenli olarak siber güvenlik denetlemeleri ve testleri yapmak.

Muhabere ve Elektronik Bilgi Sistemleri (MEBS) Destek Komutanlığı, Haziran 2012'de TSK Siber Savunma Merkezi Başkanlığı'nın kurulmasıyla takviye edilmiştir. Daha sonra Başkanlık Ağustos 2013'te MEBS ve Siber Savunma Komutanlığı olarak yeniden düzenlenmiştir . MEBS ve Siber Savunma Komutanlığı'nın yaklaşık 30 personel ile faaliyet gösterdiği, albaylık seviyesinde komuta edildiği, 7/24 usulüne göre çalıştığı ve temel olarak siber saldırılara yanıt verdiği ve TSK ağ ve sistemlerini test ettiği basında yer almıştır .

TSK'nın siber komuta konusunda küresel yaklaşımdan çok daha farklı bir yaklaşıma sahip olduğu anlaşılmaktadır. Sonrasında basına yansıyan haberlere bakıldığında Komutanlığın TSK'nın altyapısını korumak amacıyla istihbarat topladığı da anlaşılmaktadır. Siber Savunma Komutanlığının bir üyesinin değerlendirmeleri ışığında TSK'nın siber güvenlik yönetimini üç katman halinde yapılandırdığı anlaşılmaktadır. Bu hiyerarşinin en üst aşamasında politika ve karar alma süreçlerinden sorumlu olan TSK Siber Savunma Yönetim Kurulu bulunmaktadır. İkinci seviyede yer alan TSK Siber Savunma Komutanlığı ise üçüncü seviyedeki Genel Kurmay Başkanlığı ile Kuvvet komutanlıkları ve Sahil Güvenlik Komutanlığı ve Jandarma Genel Komutanlığı Siber Birimlerini yönetmektedir.

TSK'nın yürüttüğü askeri siber operasyonların temel sorunu asimetrik saldırılara simetrik ve hiyerarşik bir yapıyla karşılık verilmeye çalışılmasıdır. TSK, kara, deniz ve hava merkezli angajman stratejilerine odaklı bir yapılanma olması nedeniyle çeşitli sorunlarla karşı karşıya kalmaktadır. Bunun önüne geçilerek daha güçlü bir duruş sergilenebilmesi için TSK'nın hibrit tehditlere dinamik biçimde cevap verebilecek yeni bir yapılanmayı tasarlaması ve bununla uyumlu yeni stratejiler geliştirmesi gerekmektedir. Bu bağlamda TSK Siber Savunma Komutanlığı'nın sorumluluklarının ve ulusal siber

güvenlik yapılanması içindeki rolünün açık bir biçimde tanımlanmamış olması da sorun yaratmaktadır. Bu muğlaklığın yanı sıra, TSK'nın yüklenicilerin oynadıkları rolü ve sosyal mühendisliği hafife aldığı da söylenebilir. Oysa yükleniciler üzerinden hackerlara ve kullandıkları yazılım ile donanım hakkında bir takım bilgi ve referanslara ulaşmak mümkün olabilir. TSK'nin personel yönetimi politikası da Siber Savunma Komutanlığında deneyim kazanmaya engel bir görünüm sergilemektedir. Tecrübeli siber güvenlik personelini komutanlıkta tutmak için, TSK personel yönetimi politikasını ve de özel sektörle rekabet edebilmek için sağladığı maaş ve imkanları gözden geçirmelidir. TSK, uzun vadede, genç ve parlak beyinleri kendi hizmetine nasıl çekebileceğini düşünmelidir.

Bunun yanı sıra TSK 2014'te Siber Güvenlik konusunda bir Proje Tanımlama Dokümanı hazırlamış ve bu belge Milli Savunma Bakanlığı tarafından onaylanmıştır. Bu belgeye göre TSK Siber Komutanlığı için sadece milli yazılım ve donanım tedarik edecek ancak bu yazılım ve donanım NATO ile ortak tatbikatlarda kullanılmaya uygun olacaktır[47]. Siber Komutanlık, Türkiye'nin NATO'nun 17-21 Kasım 2014 tarihleri arasında düzenlediği Siber Koalisyon 2014 tatbikatına katılımını koordine etmiş ve tatbikatta yer almıştır[48]. Söz konusu belgede ayrıca Muhaberat ve Siber Güvenlik Komutanlığı'nın personel sayısının 80'e çıkartılarak genişletileceği de belirtilmiştir[49].

D) Emniyet Genel Müdürlüğü'nün Siber Güvenlik Yapısı

Emniyet Genel Müdürlüğü (EGM) ilk Bilgisayar Suçları ve Bilgi Güvenliği Kurulu'nu Nisan 1998'de kurmuştur. Bu kurul, bilişim suçlarının kapsamının belirlenmesi, ulusal ve uluslararası mevzuatın incelenmesi, bilişim teknolojilerinin kullanılmasıyla işlenecek suçların çeşitleri ve araçları arasındaki farklılıkları belirlenmesi ve EGM'deki birimlerin görevlendirilmesi amacıyla Mart 1999'da kurulan Bilgi Suçları Çalışma Grubu'na ön ayak olmuştur[50]. Ancak EGM bu grup kurulmadan önce de siber suçlarla mücadele etmekteydi – buna 1997'de ülkenin ilk blog yazısı yargılaması da dahildir. Bu davada sanığın bir blog sayfasında polis şiddetini eleştirmesi başka bir şahıs tarafından polise ihbar edilmiş ve sonrasında sanık terörle mücadele ekipleri tarafından tutuklanmıştır[51]. Sanık Türk Ceza

---

[47] Radikal (2014, Mayıs 27) "TSK'da siber ordu için önemli adım"

[48] USOM ve TÜBİTAK tarafından 30 Ocak 2015 tarihinde Ankara'da düzenlenen Kurumsal SOME Etkinliği sunumu. 14 Nisan 2015 tarihinde aşağıdaki bağlantıdan erişilmiştir: https://www.usom.gov.tr/faydali-dokuman/15.html

[49] Haber7.com (2013, Aralık 5) "TSK'ya Siber Savunma Komutanlığı" 26 Ağustos 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://www.haber7.com/guncel/haber/1102379-tskya-siber-savunma-komutanligi

[50] Türkiye Bilişim Şurası internet sayfası (2002, Şubat 19) "Bilişim Suçları Çalışma Grubu" 15 Eylül 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: www.bilisimsurasi.org.tr/dosyalar/9.doc

[51] "İlkiz, F. (2001, Aralık 05) "İnternet Ortamındaki Yayınlarda İki Olay ve İki Mahkumiyet Kararı ve Yasal Çalışmalar Üzerine Görüşler" Türkiye Bilişim Şurası internet sayfasından 20 Eylül 2014tarihinde aşağıdaki bağlantıdan erişilmiştir: www.bilisimsurasi.org.tr/dosyalar/45.doc

Kanunu'nun 159/1 sayılı "devletin emniyet muhafaza kuvvetlerini alenen tahkir ve tezyif" suçlamasıyla yargılanmış ve mahkum edilmiştir.

2011 senesinde EGM siber suçlarla mücadeleye odaklanan, Bilişim Suçlarıyla Mücadele Daire Başkanlığı'nı kurmuştur (birim Şubat 2013'te Siber Suçlarla Mücadele Daire Başkanlığı olarak yeniden adlandırılmıştır). Yakın dönemde bu birimin adı, Hacking Team isimli bir İtalyan firmasıyla kanun dışı telefon dinleme ve takip yapılması için anlaştığı iddiasıyla Türk medyasında yer bulmuştur.[52] Raporlara göre, EGM firmayla ilk olarak 2011'de iletişime geçmiş ve yıllar içerisinde sözleşmesini yenilemeye devam etmiştir. Sözleşmenin son yenilenmesi 2015 senesinin Şubat ayında olmuştur.[53] İddialara göre EGM şu ana kadar firmaya 440.000 Euro ödemiş ve karşılığında donanım, eğitim ve uzaktan kontrol ve veri enjeksiyonu yazılımı almıştır.

E) İstihbarat ve İstihbarata Karşı Koyma

Siber uzayın muğlaklığı güvenlik kavramlarını da etkilemektedir. Siber espiyonaj, siber casusluk ve siber istihbarat gibi kavramlar benzer anlamları nedeniyle sıklıkla birbirinin yerine kullanılmaktadır. Aslında, bunların tamamı benzer saldırı yöntem ve benzer teknolojilere bağlıdırlar. Ancak, siber saldırının failinin bir devlet mi yoksa örgüt mü olduğunu bulmak zorlu bir meseledir. Devletlerin siber uzayın belirsizliğini ya da sahipsizliğini kendi çıkarları için kullanmaktadırlar. Siber istihbaratın en dikkati çeken yönü siber güvenlik tehditlerine yanıt verebilmek amacıyla çeşitli siber araçlarla bilgi toplamaktır.

Milli İstihbarat Teşkilatı (MİT), Türkiye'deki siber güvenlik tehditlerinin gerçekleşmeden engellenmesi için gerekli istihbaratı toplamaktan sorumlu birimlerden biridir. MİT'e bu alanda yetkiler veren 6532 sayılı "Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun" TBMM'ce 17 Nisan 2014'te yasalaştırılmış ve Cumhurbaşkanı onayladıktan sonra 26 Nisan 2014'te yürürlüğe girmiştir. Bu yeni yasa MİT'in görev ve sorumluluklarını şu şekilde yeniden tanımlamaktadır:

"Dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak."

[52] Radikal (2015, Temmuz 12) "'Hacker skandalı'nda ilginç ortaklık MHP kasetlerine kadar uzandı"
[53] Hürriyet (2015, Temmuz 9) "Polise faturalı hackerlık hizmeti"

Yapılan kanun değişikliğinin MİT'in kurumsal altyapısında nasıl bir değişiklik yarattığına dair açık bir bilgi olmamakla birlikte son dönemlerde Teşkilat tarafından verilen iş ilanları iş bölümünde meydana gelen değişiklikler hakkında bazı ipuçları vermektedir. MİT'in iş ilanları sitesinden şu alanlarda çalışmak üzere uzmanlar arandığı anlaşılmaktadır: Sinyal Analizi ve Uygulamaları, Şifreleme ve Kripto Analizi, Siber Faaliyetler , Uydu İletişimi, Coğrafi Bilgi Sistemleri (GIS), İşitsel-Görsel Data İşleme, Telekomünikasyon Sistemleri, Yazılım Geliştirme, İletişim Yazılımı Geliştirme, Donanım Geliştirme, Mobil Uygulama Geliştirme, Sistem Yönetimi, Ağ Yönetimi, Veri tabanı Yönetimi, Bilgi Güvenliği ve Internet Teknolojileri, Sistem Analizi, Mekanik Sistem Tasarlama, Sistem Desteği ve Eğitimi, Veri İşleme. Tüm bu uzmanlık talepleri MİT'in kurumsal yapısının siber istihbarat çerçevesi kurmak yönünde yeniden yapılandırıldığına işaret etmektedir.

6532 sayılı kanun değişikliğinden sonra, dönemi Başbakanı Tayyip Erdoğan yaptığı açıklamada TİB'in yeniden yapılandırılacağını ve bu görevin de MİT'e verildiğini belirtmiştir. Nitekim TİB'in başına MİT'in desteğiyle eski bir MİT çalışanı olan Ahmet Cemalettin Çelik başkan olarak atanmıştır. Bu son atama TİB ile MİT'in siber izleme de dâhil olmak üzere siber güvenlik konularında yakın işbirliği içinde faaliyet gösterdiklerine dair açık bir ipucu vermektedir. Ancak, bu yakın işbirliğinin Türkiye'de siber güvenlik farkındalığını artırdığı ve gerçek anlamda bir siber savunma faaliyetini beraberinde getirdiği söylenemez.

F) Yakın Dönemdeki Gelişmeler

2013 senesinin sonunda Türkiye sızdırılan tapeler ve telefon konuşmalarıyla ortaya çıkan bir yolsuzluk skandalıyla sarsılmıştır. Müteakip aylarda pek çok sayıda ses kaydı, ki bunların arasında Dışişleri Bakanlığı'nda yapılan oldukça hassas ve yüksek seviyeli bir toplantıdan alınan kayıtlar da bulunmaktadır, yayınlanmıştır ve bu kayıtların menşeinin araştırıldığı soruşturmalar 2014 senesinin başında TÜBİTAK ve Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi'ne (BİLGEM) uzanmıştır. Aralarında TÜBİTAK başkan yardımcısı ve BİLGEM başkanı Hasan Palaz'ın da TÜBİTAK çalışanlarının kaydadeğer bir kısmı görevlerini kaybetmiştir. Palaz, soruşturmaya dair yazdığı kitabında 2014'ün ilk çeyreğinde TÜBİTAK idari personelinin yüzde 80'inin işten atıldığı ya da siyasi sebeplerle istifa etmeye zorlandığını iddia etmektedir.[54] 2015'e gelindiğinde, bu sayı 1000'den fazla bilim adamı ve araştırmaya erişmiştir. Bir diğer deyişle, TÜBİTAK çalışanlarının dörtte biri işlerinden ayrılmıştır. Palaz bunun TÜBİTAK'ta ciddi bir kabiliyet ve uzmanlık kaybına yol açtığını savunmaktadır. Nitekim 2015 senesinin Mart ayında BİLGEM yasadışı bir örgütün yargılandığı bir davada delil olarak sunulan ve kuruma analiz etmesi talebiyle iletilen dört sabit diski kurumda "dijital analiz incelemesi

[54] Palaz, H. (2015, Mart) "Ömrümü Yedin Bay Böcek!" Cinius Yayınları ss.184-185

yapabilecek personel ekibinde son altı ay içerisinde yaşanan yoğun değişim sebebi ile söz konusu [talebe] yönelik uygun ve ehliyetli personel [bulunmadığı]" gerekçesiyle geri çevirmiştir.[55]

6 Şubat 2014 tarihinde Meclis 6518 sayılı torba yasayı onamıştır.[56] Yasayla 4 Mayıs 2007 tarihli ve 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"[57] üzerinde bazı değişiklikler yapılmıştır. Yeni torba yasa ile TİB ulusal siber güvenlik faaliyetleri çerçevesinde içerik, yer ve hizmet sağlayıcılar ile diğer ilgili kurum ve kuruluşlar arasında siber saldırıların tespit edilmesi ve önlenmesi konusunda koordinasyon sağlamakla görevlendirilmiştir. Torba yasa ayrıca 5 Kasım 2008 tarihli, 5809 sayılı Elektronik Haberleşme Kanunu'nda da değişiklikler yapmıştır.[58] Bu değişikliklerle birlikte, BTK "siber güvenlik ve internet alan adları konularında Bakanlar Kurulu, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirme"[59] sorumlulukları verilmiştir. Torba yasanın 106. maddesiyle Siber Güvenlik Kurulu siber güvenlik üzerine politikaların, stratejilerin ve eylem planlarının onaylanmasıyla görevlendirilmiştir. Siber Güvenlik Kurulu bu politikaların, stratejilerin ve eylem planlarının ülke çapında etkin bir biçimde uygulanması için gerekli kararları almak, kritik altyapıların belirlenmesi konusundaki tavsiyelerde son kararı vermek, siber güvenlik konusundaki düzenlemelerin bir kısmından veya tamamından muaf olacak kurum ve kuruluşları belirlemek ve yasa tarafından belirlenen diğer görevleri yerine getirmekle sorumlu tutulmuştur. Değişiklik ile Siber Güvenlik Kurulu'nun çalışma usul ve esasları Başbakanlık tarafından yayınlanacak yönetmeliklerle belirlenecektir.

Zaman içerisinde TİB'in siber güvenlik alanında yetkileri ve sorumlulukları da artmıştır. 2015 senesinin Mart ayında kabul edilen bir değişiklik TİB'e "yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya bir kaçına bağlı olarak hâkim veya gecikmesinde sakınca bulunan hâllerde, Başbakanlık veya millî güvenlik ve kamu düzeninin korunması, suç

[55] Radikal (2015, Mart 08) "TÜBİTAK'ta dijital analiz yapacak eleman kalmamış!"
[56] "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun", 19 Şubat 2014 tarihli 28918 sayılı Resmi Gazete
[57] 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 04 Mayıs 2007
[58] 5809 sayılı Elektronik Haberleşme Kanunu 05 Kasım 2008, 10 Kasım 2008 tarihli 27050 sayılı Resmi Gazete
[59] "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun" Madde 103, 19 Şubat 2014 tarihli 28918 sayılı Resmi Gazete

işlenmesinin önlenmesi veya genel sağlığın korunması ile ilgili bakanlıkların talebi"[60] hallerinde "internet ortamında yer alan yayınla ilgili olarak içeriğin çıkarılması ve/veya erişimin engellenmesi" kararını vermek yetkisini sağlamıştır. Bu süreçte TİB, içerik çıkarılması veya bir sayfaya erişimin engellenmesi kararını verdikten sonra ilgili erişim, içerik ve alan sağlayıcıyı bilgilendirir ve sağlayıcıların da dört saat içerisinde talebi yerine getirmeleri gerekmektedir. Kanuna göre TİB'in kararının yerine getirilmemesi 50.000 ila 500.000 TL (19,000-190,000$) idari para cezasıyla cezalandırılır.

TİB'in aynı zamanda karar aldıktan sonra onay için 24 saat içerisinde sulh ceza hakimine başvurması gerekir; hakimin ise kararını TİB'in başvurusunu aldıktan sonra 48 saat içerisinde vermesi gerekir. Hakim TİB'in kararını onaylamazsa engelleme otomatik olarak kaldırılır. Diğer yandan eğer hakim TİB'in içerik veya internet sayfalarına erişim engelleme kararını onaylarsa, içerik, hizmet ve erişim sağlayıcılarının "suçların faillerine ulaşmak için gerekli olan bilgiler[i]" hakim kararı üzerine adli mercilere sunması gerekir ve aksi takdirde para cezasıyla karşı karşıya kalırlar.[61] Erişim sağlayıcılarının TİB'in kararlarına uymak için gerekli tüm yazılım ve donanımı kendileri tedarik etmesi gerekir ve erişimin engellendiği yayınlara alternatif erişim yöntemlerine karşı önleyici tedbirler almaları gerekir.[62] Kanun Erişim Sağlayıcıları Birliği'nin (ESB) kurulmasını sağlamıştır. Bu birliğe katılım TİB'in kararlarına ve kanuna uyumu sağlamak için mecbur kılınmıştır. Birlik üyelerinin TİB'in kararlarına uymak için gerekli tüm yazılım ve donanımı tedarik etmeleri zorunludur. Özetle 2015'te yapılan değişikliklerle TİB içeriğe ve internet sayfalarına erişimi hızlıca sağlama yetkisi kazanmış ve kararlarına uyulmasını sağlamak için güçlü mali ve yasal caydırıcılar elde etmiştir.

II. Devlet Dışı Aktörler: Yerli Hacker Grupları ve Saikleri

Türkiye menşeli hackerlar uluslararası siber saldırılarda da rol oynamaktadırlar. Ancak bu grupların profilleri hakkında gelecekte kaynak olarak kullanılabilecek hiçbir araştırma yoktur. Türk hackerların kabiliyetlerinin anlaşılması ülke içinden kaynaklanan tehditlerin anlaşılabilmesi için elzemdir. Son yıllarda devletler, alışılagelmiş internet altyapısını değiştirerek, bağlanabilirliğin kısıtlanması ve intranet bağlantıların kullanılmasına imkan verilmesi fikirlerine destek vermeye başlamışlardır.

Aşağıdaki özellikler Türkiye'deki tipik bir hackerı betimlemektedir:

---

[60] 5651 Sayılı Kanun Madde 8/A (27 Mart 2015 tarihinde yapılan değişiklik – 6639/29) Aşağıdaki bağlantıdan erişilebilir: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

[61] 5651 Sayılı Kanun Madde 10 (2007, Mayıs 4) 23 Mayıs 2007 tarihli 26530 sayılı Resmi Gazete

[62] 5651 Sayılı Kanun Madde 6/Ç (6 Şubat 2014 tarihinde yapılan değişiklik – 6518/89) Aşağıdaki bağlantıdan erişilebilir: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

- 14-45 yaşlar arasında ama ekseriyetle 18-25 yaş aralığındadırlar
- Çoğunlukla lise ya da üniversite mezunudur ancak hepsi bilgisayar bilimi mezunu değildir
- Yeni hackerlar kabiliyetlerini hacker forumlarından öğrenerek elde ederler ve çoğunlukla basit hackleme araçları kullanırlar
- %92'si erkek, %8'i kadındır
- Çoğunlukla orta veya düşük gelir seviyeli ailelerden gelirler
- Sosyal Mühendislik[63] ve Ters Mühendislik[64] saldırılarını tercih ederler
- Ufak bir grup uydu verisi takibi, istihbarat gibi konularla ilgilenmektedir[65]

Türkiye'de internetin sivilleşmesiyle birlikte birkaç hacker grubu ortaya çıkmaya başlamıştır. Bu bölümde bu gruplardan yedi tanesine odaklanılacaktır: Ayyıldız, RedHack, B3yaz Hacker, Turk Hack Team, Cyber Warrior (Akıncılar), Türk Güvenliği ve PKK Hack Team.

A) Ayyıldız Tim

İnternet sitelerine göre Ayyıldız Tim 2002 yılında kurulmuştur. Grup hedeflerini yedi maddede sıralamıştır:

> *"1-Türkiye Cumhuriyeti Devletine,Tüm Kamu Kurum ve Kuruluşlarına yönelebilecek her türlü saldırıyı bertaraf etmek.*
>
> *2-Türkiye karşıtı,Satanist,Pornografik,Anayasal düzeni değiştirmeye yönelik yayın yapan sitelerin,sistemlerin yayınlarını durdurmak.*
>
> *3-Faydalı yayın yapan sitelere ve sistemlere gereken teknik desteği vermek.*
>
> *4-Gov.tr,pol.tr,edu.tr,bel.tr gibi Türkiye Cumhuriyeti Devletini İnternette Temsil eden sistemleri korumak.*

---

[63] "Sosyal Mühendislik: Crackerların, normalde kapalı olan bir ağa erişim sağlamak amacıyla ağa erişimi olan kişileri kandırmak için sosyal bir durum tasarladıkları ya da "mühendisliğini yaptıkları" ya da kişileri aslında var olmayan bir gerçekliğe inandırdıkları aldatmaya dayalı süreç. Bilgisayar sistemlerini kırmak için crackerlar sıklıkla gelişmiş sosyal mühendislik yeteneklerini kullanırlar. Sosyal mühendislik vakalarının iyi bir derlemesine Kevin Mitnick'in The Art of Deception kitabında erişilebilir." *Webster's New World Hacker Dictionary*, Indianapolis: Wiley Publishing, 2006, s. 293.

[64] "Ters mühendislik: Bir bilgisayar sisteminin parçalarının ve parçalarının birbirleri arasındaki ilişkilerinin belirlenebilmesi için analiz edilmesini içermektedir. Ters mühendislik sıklıkla bir sistemin uzun süre kullanılabilirliğini sağlamak için yeniden tasarlanmasını sağlamak amacıyla ya da orijinal tasarıma erişim olmadan bir sistemin taklitlerini üretebilmek için yapılır. *Webster's New World Hacker Dictionary*, Indianapolis: Wiley Publishing, 2006, s. 269.

[65] Ufuk Eriş, "Türkiye'de Kırıcı (Hacker) Kültürü", Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Doktora tezi, Kasım 2009, ss. 141-200.

5-Karşı propaganda faaliyetleri yürüterek Türkiye Cumhuriyet Devletinin Manevi şahsını dünya milletleri arasında hak ettiği yere getirmek.

6-Gereken hallerde(Yönetim Kurulu Kararı)Ülkemize yönelen sözlü,yazılı ve fiili saldırılara şiddetle cevap vermek.

7-Kamuoyunun bilinçlenmesi adına İnformation admin eli ile yazılı açıklamalar yapmak."[66]

Ayyıldız Tim'in crackleme faaliyetlerine dair Zone-H[67] internet sitesinde 13.579 tane duyuru vardır. Zone-H tarafından kayıt altına alınan tahrif edilmiş sitelerden birisinde Ayyıldız Tim kendilerini aşağıdaki not ile Türkiye'nin Siber Ordusu ilan etmişlerdir:

"*Biz Türkiye'nin sanal ordusuyuz.*

Vatanımız için düşmanlar ile soğukta, karda, kışta nasıl savaşıyorsak sanal alemde de vatanımız uğruna savaşırız.

Asla yorulmaz. Asla pes etmeyiz. Birbirimizi destekler, iyi gününde kötü gününde hep bir oluruz.

Dinimize ve Türklüğe karşı kötü fikirlere sahip olan tüm devletlere sanal savaş açacağız.

Bu kötü fikirlere devam edecekseniz sanal savaşa hazır olun! Kimseden korkmayız!

Gerektiği yerde gereken cevabı veririz!

AYYILDIZ TiM

TURKiYE'NiN SiBER ORDUSU"[68]

Bu satırlarda ve ilkelerinde görüleceği gibi Ayyıldız çoğunlukla devlet hedefleriyle işbirliği yapan ya da paralel bir hatta çalışan kendi ifadesiyle vatansever bir hacker grubudur.[69] Ancak Ayyıldız Tim'in altı üyesi site sahiplerine şantaj yaptıkları gerekçesiyle tutuklanmıştır. Ayyıldız Tim bu şahısların üyeliğini inkar etmiştir. Ancak grubun eylemleri ve suç unsuru teşkil eden faaliyetlerle bağlantılarına dair bazı şüpheler vardır.[70] Bu şüphelerin yanı sıra Ayyıldız Tim saldırılarında çoğunlukla devletçi bir duruş

[66] Ayyıldız Tim Misyonu, http://www.ayyildiz.org/navigasyon.php?id=22 (21 Ağustos 2015 tarihinde erişilmiştir)
[67] Zone-H tahrif edilmiş internet sitelerinin arşivini tutan ünlü sitelerden biridir. Site yönetimi sahte kayıtları önlemek için tahriflerin gerçek olup olmadığını kontrol etmektedir. Hackerların tahriflerine dair kanıtı Zone-H internet sitesine iletmektedir. Böylelikle eylem geçmişlerini ve namlarını arttırmaktadırlar. Daha fazla bilgi için bkz; http:// http://www.Zone-H.org/
[68] Ayyıldız Tim, "http://www.simos1.gr", Zone-H, http://www.Zone-H.org/mirror/id/13249689, 15 Mart 2011.
[69] Ayyıldız – Tim, Görünmeyen Kahramanlar (Sanal Alemin Askerleri), Ankara, 2008, s. 16.
[70] Elvan Ezber, "Ayyıldız Tim'e Polisten Çete Baskını". Radikal, 12 Ağustos 2011, http://www.radikal.com.tr/turkiye/Ayyıldız_time_polisten_cete_baskini-1059754; Elvan Ezber, "Ayyıldız Tim: Bekir K. ile bağlantımız yok". Radikal, 14 Ağustos 2011,

sergilemiştir. Özellikle Anonymous'un Türkiye'ye yakın dönemde kitle halinde yaptığı saldırılara karşı Ayyıldız Tim'in Türkiye'yi savunması da, bu grubun Türkiye'nin gelecekte kurulacak nükleer tesisinin siber güvenliğine bir tehdit teşkil etmeyeceğini kanıtlamıştır.[71]

B) RedHack

RedHack Türkiye'deki en bilinen hacker gruplarından biridir. Röportajlarının birisinde grubun lideri RedHack'in 1997 senesinin Mayıs ayında kurulduğunu iddia etmiştir.[72] RedHack ideolojisini, eşit, adil ve sömürünün olmadığı bir dünya için hacklemeyi kullanmak olarak açıklamıştır.[73] RedHack aynı zamanda konumunu "[faşist] düzene kurşun atan her örgütün emrinde"[74] olarak belirtmiştir.

Zone-H internet sitesinde 2008'den başlayarak RedHack'e atfedilmiş bazı tahrif kayıtları mevcuttur.[75] Hack grubu Ankara Emniyet Müdürlüğü'nün internet sitesine yaptıkları ilk saldırıdan ve ardından Türk kamuoyuna yaydıkları gizli belgelerle üstüne daha çok ilgi çekmeye başlamıştır.[76] Grup 2013'de Gezi Parkı protestolarının ardından devlet kurumlarına yaptıkları şiddetli saldırılardan sonra popülerlik kazanmıştır.[77] Başka bir saldırıdan sonra RedHack Ankara Emniyet Müdürlüğü'nde görev yapan polis memurlarının email hesap ve şifre bilgilerini yayınlamıştır. RedHack, bu saldırıların yanı sıra Emniyet Genel Müdürlüğü, Türk Futbol Federasyonu, Milli İstihbarat Teşkilatı, Türk Telekom, Hava Kuvvetleri Komutanlığı, Türk Hava Yolları, Yüksek Eğitim Kurumu ve Dışişleri Bakanlığı'nın sitelerini tahrif etmiş ve elde ettiği diplomatik görev mensuplarının kimlik bilgileri ve devlet kurumları arasındaki gizli iletişimler gibi gizli belgeleri yayınlamıştır.[78] RedHack'in uluslararası hacker gruplarıyla işbirliği yapma kapasitesi vardır. 2013 senesinde RedHack ve Anonymous birlikte çalışarak İsrail İstihbarat Servisi'ne (MOSSAD) bir saldırı düzenlemişlerdir.[79]

---

[71] Gamze Akkuş, "Anonymous resmi hedefe saldırdı. Ayyıldız Tim karşı atakla cevap verdi". Hürriyet, 10 Haziran 2011, http://www.hurriyet.com.tr/ekonomi/17996737.asp

[72] "Kızılhack hedefimiz ezenler", Atılım, 21 Eylül 2006, http://web.archive.org/web/20100507133839/http://www.atilim.org/atilim/modules.php?name=Guncel&file=article&sid=16899 (3 Mayıs 2015 tarihinde erişilmiştir)

[73] A.g.e.

[74] A.g.e.

[75] Daha fazla detay için bkz. "RedHack Defacements", Zone-H, http://www.Zone-H.org/archive/notifier=RedHack/page=1 (2 Mayıs 2015 tarihinde erişilmiştir)

[76] Serkan Ocak, "Ankara Emniyeti Çökertildi", Radikal, 28 Şubat 2012, http://www.radikal.com.tr/turkiye/ankara_emniyeti_cokertildi-1080108 (3 Mayıs 2015 tarihinde erişilmiştir)

[77] "RedHack Emniyeti hackledi mi?", Milliyet, 05 Eylül 2013, http://www.milliyet.com.tr/RedHack-emniyet-i-hackledi-mi-/gundem/detay/1759446/default.htm (Accessed on 5 May 2015)

[78] Tahriflerin kronolojisiyle ilgili daha fazla bilgi için bkz; Burak Polat, Cemile Tokgöz Bakıroğlu, Mira Elif Demirhan Sayın. "Hacktivism in Turkey: The Case of RedHack", Mediterranean Journal of Social Sciences, Vol 4, Ekim 2013.

[79] Yiğit Turak, "RedHack özelinde Siber olaylar ve Siber Suçlar", İstanbul Bilgi University, Unpublished Course Project for Cyber Crimes and its Practice in Turkish Law, http://www.yigitturak.com/wp-content/uploads/RedHack-Özelinde-Siber-Olaylar-ve-Siber-Suçlar.pdf (11 Mayıs 2015 tarihinde erişilmiştir)

C) B3yaz Hacker

Bu hacker grubu beyaz hackerlara, yani çevrimiçi sistemleri daha güvenilir hale getirmek için üreticilere güvenlik açıklarını bildiren zararsız hackerlara bir referans olarak isminde Türkçe beyaz kelimesini farklı bir yazılışıyla kullanmıştır. Grup, B3yaz Hacker'ın internet sayfasında kadrolarının Pentest[80] taleplerine hazır olduğunu ilan etmiştir. Bu, Türkiye'de bir hacker grubunun gerçek bir Pentest hizmeti için hackleme kabiliyetlerini sunduğu tek örneği teşkil etmektedir. Sızma testleri güvene dayalı olduğu için, firmalar, firmanın hassas bilgilerini koruma garantisi verebilecek güvenilir özel güvenlik firmalarını tutmayı tercih ederler.

B3yaz Hacker'ı saldırıları iki gruba ayrılabilir. İlk saldırı grubu internet sitelerine güvenlik açıklarını bildirmek için yapılanlardır. İkinci olarak ise grubun değer yargılarına aykırı içerik paylaşan internet sitelerine yapılan saldırılar vardır. Zone-H'de, B3yaz.org, B3yaz, B3yazHacker adları altında kayıtlar vardır; bunlar, çoğu 2015 senesinde farklı internet sitelerine yapılmış olan toplam 540 adet tahriften oluşmaktadır. B3yaz Hacker grubunun kabiliyetleri incelendikten sonra, B3yaz Hacker'ın Türkiye'nin kritik altyapısı ve nükleer enerji tesisleri açısından bir tehdit olarak değerlendirilmeyeceğini söylemek mümkündür.

D) Turk Hack

Turk Hack Türkiye'deki en teşekküllü ve iyi bilinen hacker gruplardan biridir. Turk Hack Team 2002'de kurulmuştur.[81] İnternet siteleri hacker gruplara göre en düzenli internet sitelerinden birisidir; tarihçeden videolara, eğitimden e-kitaplara kadar birçok bölümü vardır. İnternet sitesinin tasarımı, Turk Hack yönetiminin bir topluluk kurup bunları internet sitesi aracılığıyla eğitmeyi hedeflediklerini göstermektedir. Son on yıl boyunca grup milliyetçi çizgisini korumuştur ancak artık dini imalara da yer vermektedir. Üyeleri grubu "Vatanını seven Müslümanlar" olarak tanımlamaktadırlar.

Grubun ilan ettiği hedefleri aşağıdakilerden oluşmaktadır:

"1. Dilimize, dinimize, ülkemize, inançlarımıza, örflerimize, adetlerimize, toplum ahlakına ve bunlar gibi değerlere, aykırı yayın yapan sitelerin hayatına son vermektir.

2. Hack'in zevk için değil misyon için yapılacağını aşılamaktır.

---

[80] Pentest İngilizce sızma testinin (penetration testing) kısa yazılışıdır. "Sızma Testi (genel terim): Güvenlik açıklarının ve crackerların bunları ne ölçüde kendi avantajlarına kullanabileceğinin araştırıldığı ve belirlendiği süreç. Bir kuruma ait, bilgisayarların, ağ birimlerinin ve uygulamalarının da içinde bulunduğu bilişim sistemlerinin güvenlik vaziyetinin değerlendirilmesi için kritik önem teşkil eden bir araçtır. *Webster's New World Hacker Dictionary*, Indianapolis: Wiley Publishing, 2006, s. 243.

[81] http://pastebin.com/mFFw5DqS (3 Ekim 2015 tarihinde erişilmiştir)

3. Doğru, dürüst, ahlaklı ve yararlı yayın yapan sitelere yardımcı olmak ve onlara çıkar gözetmeden destek olmaktır.

4. Turk Hack Team Türk Vatanı için çalışır

5. Bu misyonu kabul eden Turk Hack Team üyelerine sorunları ile yardım için hiç bir şart gözetilmeyecektir."[82]

Turk Hack Team faal olan en büyük botnetlerden birisini kontrol ettiklerini iddia etmektedir. Zone-H internet sitesinde Turk Hack Team'in farklı yazılışlarıyla birçok kaydı vardır, bu da kabiliyetlerini tam olarak anlamayı güçleştirmektedir. Ancak yakın dönemde Turk Hack Team'in lideri Zorrokin'in, Papa'nın Ermeni meselesi hakkındaki açıklamasından sonra Kutsal Makam'ın internet sitesine yaptığı saldırı grubun yetkinliği ve potansiyeli hakkında bazı fikirler vermektedir.[83] Grubun son saldırısı 7 Haziran 2015 Türkiye genel seçimlerinden hemen önce *New York Times* gazetesinde Türk cumhurbaşkanının eleştirildiği bir makalenin yayınlanmasının ardından gazeteye yapılan saldırı olmuştur. Saldırı homedelivery.nytimes.com, es.nytimes.com, blog.nytimes.com, app.nytimes.com, register.nytimes.com adreslerini durdurmuş ve hosting sunucuna zarar vermiştir.[84] Bu saldırının akabinde Turk Hack Team yine Türkiye cumhurbaşkanını eleştiren *The Guardian* gazetesine saldırmış ve gazetenin internet sitesini ve sunucusunu kısıtlı olarak kesintiye uğratmıştır.[85] Tüm bu saldırılar grubun kabiliyetleri konusunda ipuçları vermektedir. Bu grubun hükümet yanlısı eğilimleri, Türkiye'nin planlanan nükleer enerji tesislerine muhtemel bir tehdit unsuru olmayacağını göstermektedir.

E) Cyber Warrior (Akıncılar)

Cyber Warrior, diğer adıyla Akıncılar[86], 1999'da illegal-port adıyla kurulmuş bir gruptur. Daha sonra grubu Cyber Warrior olarak yeniden yapılandırmışlardır. Grubun hiyerarşisi ordu hiyerarşisiyle

---

[82] Bkz. http://www.turkhackteam.org/misyon.html (12 Haziran 2015 tarihinde erişilmiştir)
[83] "Vatikan'a Turk Hack Team saldırdı", Aydınlık, 15 Nisan 2015, http://www.aydinlikgazete.com/bilimteknoloji/vatikan-a-turk-hack-team-saldirdi-h67740.html (15 Mayıs 2015 tarihinde erişilmiştir)
[84] "New York Times hacklendi", Sabah, 28 Mayıs 2015, http://www.sabah.com.tr/gundem/2015/05/28/new-york-times-hacklendi (6 Haziran 2015 tarihinde erişilmiştir)
[85] "Türk Hackerlardan Müdahale", Milliyet, 05 Haziran 2015, http://www.milliyet.com.tr/turk-hackerlardan-the-guardian-gazetesine-istanbul-yerelhaber-824596/ (11 Haziran 2015 tarihinde erişilmiştir). Ayrıca bkz; http://www.turkhackteam.org/basin-duyurusu/1139755-guardian-operasyonu-ulusal-basinda.html
[86] Osmanlı İmparatorluğu'nda düşmanı ön saldırılarıyla şaşırtan ve düşman topraklarında keşif görevi yapan özel bir askeri birlik.

aynıdır. Eskiden yaptığı bir gönüllü toplama çağrısında grup kendisini bir kardeşlik yolu olarak tanımlamıştır.[87]

Üyelerinde aranan özelliklerini şöyle sıralamışlardır[88]:

- Din, örf, adet, ananelerimize sadık
- Türk Milliyetçileri
- Birlik üyeleri arasında bir kardeş bağı sağlayacak kişiler.
- Birlikteki kişiler başka bir oyuncuya küfür, argo söz, ağır laf sarf etmeyecektir. Birliğimizden birine yapılmış hakaret hepimize yapılmış sayılır.

Cyber Warrior internet sitesi grubun Türkiye İnternet yasasının (No. 5651[89]) hazırlanması sürecinde aktif olduğunu iddia etmektedir, bu da Türk karar vericilere veya siyasi elite yakın oldukları anlamına gelebilir. Türkiye'nin siber güvenlik yasasının (5651) ardından grup görevlerini İnternet Yasasına uygun olarak yeniden şekillendirmiştir:

- "TIM'in başlıca Amaç/Görevleri; İnternet üzerinden İnanç ve Ahlaki değerlerimize saldırı yapan, Saf beyinleri bulandırmaya yönelik içerikler bulunduran, Satanist ve Pornografik içerikli yayınlarla mücadeledir. Türkiye Aleyhtarı Yayınlar, Toplum ve kamu vicdanını Olumsuz Etkileyen Durumlar da (Bu Misyon'un Genel Prensibi Doğrultusunda) Misyon Kapsamındadır.
- TIM'in Genel Prensibine (Misyon'a) Uygun Yayın Yapan kurum, Site/Grup ve Oluşumlara Güvenlik ve Diğer Teknik Detaylar Hakkında, Herhangi Bir Menfaat Gözetmeksizin Güvenlik Desteği Saglanır.
- Bizim degerlerimize saldırmadığı sürece hiç bir yayın mücadele kapsamına girmez."[90]

Grup aynı zamanda internet sitelerinin kurum bölümünde görevlerini detaylandırmıştır:

- Cyber Warrior TIM'in hiç bir şekilde herhangi bir dernek, kurum, örgüt, parti, siyasal ya da ideolojik görüs ile bağı yoktur.

---

[87] http://board.tr.gladiatus.gameforge.com/index.php?page=Thread&threadID=8202
[88] A.g.e
[89] "Türk hükümeti 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu Mayıs 2007'de yürürlüğe koymuştur. Bu yasanın kabulu YouTube'dan erişilebilen ve Türkiye Cumhuriyeti'nin kurucusu Mustafa Kemal Atatürk'ü tahrif eden videolara dair kaygıların, internette çocuk pornografisi ve müstehcen içeriklerin erişilebilirliğine ve intihar ya da çocuklar için zararlı olabilecek ya da uygun olmayabilecek maddelere dair bilgi veren internet sitelerine dair artan kaygıların ardından gelmiştir." Yaman Akdeniz, (2010, Ocak 11) *Report of the OSCE Representative on Freedom the Media on Turkey and Internet Censorship*http://ec.europa.eu/enlargement/pdf/speak_up/osce_freedom_of_the_media_on_turkey_and_internet_censorship.pdf (10 Kasım 2015 tarihinde erişilmiştir)
[90] http://www.cyber-warrior.org/Misyon.asp

- TIM'e Kabul Edilen üye; Grup içinde Bilgi ve Uzmanlık Alanına Göre; Görev Organizasyonu' nda Görev Almak Üzere; Sorumlulukları ve Görev Tanımı Belirlenir ve Gruba Dahil Edilir."[91]

Cyber Warrior üyeleri bazı çevrimiçi forumlarda Türkiye'deki hiçbir internet sitesine saldırmadıklarını iddia etmişlerdir.[92] Cyber Warrior'ın davranış biçimindeki bu değişiklik, grubun Türk polisiyle farklı seviyelerde bağlantıları olduğu iddiasıyla örtüşmektedir.[93] Zone-H'te grubun 7895 tahrif kaydı vardır. Cyber Warrior mensupları diğer ülkelerin yanı sıra İsrail, Mısır, Avusturya ve Ermenistan'a saldırmışlardır.[94]

Erişilebilen tüm kanıtlar grubun devletle güçlü ilişkileri olduğunu göstermektedir.[95] HP Siber Güvenlik Araştırmaları Siber Risk Raporu 2015 aşağıdaki kanıtlara dayanarak onları devlet destekli hacker grubu olarak sınıflandırmıştır:

"Cyber Warrior ekibi tehdit aktör grubunun bir parçası olan Akıncılar hacker ekibinin üyeleri Türk polisi tarafından RedHack ve Türk veya İslami ideallere tehdit olarak algılanan diğer birimlere yaptıkları saldırılardan dolayı methedilmiştir. Akıncılar'ın bazı aktörleri Bilişim Güvenliği ve Bilişim Suçlarına Karşı Mücadele Derneği'nin yönetim kadrosundadır ve bu kurum gov.tr ve pol.tr domainlerine ücretsiz bilgi güvenliği yardımı yapmış ve devlet kurumlarına hassas bilgiler aktarmışlardır. Akıncılar mensubu Emrullah Aydemir, f0rtys3v3n rumuzu altında siyah şapka faaliyetleri[96] yürütmektedir ve Türk hükümetine bilim ve araştırma konularında danışman bir kurum olan TÜBİTAK'a güvenlik sağlamıştır.

---

[91] A.g.e.

[92] "Cyber Warrior'u ekol yapan etkenler nelerdir?", haberseyret.com, 26 Ocak 2014, http://haberseyret.com/haber/5319/cyber-warrioru-ekol-yapan-etkenler-nelerdir (1 Haziran 2015'te erişilmiştir)

[93] "En makbul milliyetçi 'hacker' olan milliyetçi", Agos, 18 Haziran 2012, http://www.agos.com.tr/tr/yazi/1714/en-makbul-milliyetci-hacker-olan-milliyetci (29 Mayıs 2015'te erişilmiştir)

[94] "İsrail Sitelerini Hackleyen Türk Hacker", http://www.dailymotion.com/video/xdk8lp_israil-sitelerini-hackleyen-turk-ha_tech (11 Haziran 2015'te erişilmiştir)

[95] "Cyber Warrior Röportaj 1. Bölüm", http://www.cyber-warrior.org/Forum/haberseyret-ile-Cyber-warrior-hk-roportaj_510091,0.cwx (02 Haziran 2015'te erişilmiştir); "Cyber Warrior Röportaj 2. Bölüm", http://www.cyber-warrior.org/Forum/haberseyret-ile-cyber-warrior-hk-roportaj-2-bolum_510137,0.cwx (02 Haziran 2015'te erişilmiştir)

[96] "Siyah şapka: Hacking cemiyetinin kötü ya da suçla ilişkili yüzü – siber suç türü. Kara şapkaların faaliyetlerinin arasında cracker'ın intikam, sabotaj, şantaj ya da açgözlülüğü sebebiyle ortaya çıkan yıkıcı bilgisayar *exploit'*leri vardır. Tabiatı itibariyle siber olmayan suçlarda olduğu gibi, Siyah Şapka *exploit'*leri mala ve/veya şahıslara zarar gelmesiyle sonuçlanabilir. Bilgisayar yeraltında, farklı çeşitlerde Black Hat'ler vardır; bunlardan en sık rastlananı, başkalarının bilgisayar sistemlerine yetkileri olmadan erişen, kopya korumalı programları çalıştırmak için kodunu karıştıran, internet sitelerinin kapasitelerini doldurarak meşru kullanıcıların erişimini engelleyen ve bilinçli olarak internet sitelerini tahrif eden "cracker"lardır." *Webster's New World Hacker Dictionary*, Indianapolis: Wiley Publishing, 2006,

Nisan 2012'de, grubun yöneticisi Gökhan Şanlı'nın da aralarında bulunduğu Bilişim Güvenliği ve Bilişim Suçlarına Karşı Mücadele Derneği temsilcileri, Beyaz Saray'ın Türkiye'deki dengi olan Çankaya Köşkü'nde düzenlenen, Türkiye'deki bazı internet sitelerine erişimin durdurulması ve entellektüel mülkiyet hakları üzerine bir toplantıya katılmıştır. Doktoray rumuzunu kullanan Şanlı, Cyber Warrior forumlarını yönetmektedir. Dogukan rumuzunu kullanan ve artık rahmetli olan Halit Uygur, Cyber Warrior TİM'de ve aynı zamanda İstanbul'daki Milli Eğitim Bakanlığı'nda kilit rol oynayan bir figürdü."[97]

Cyber Warrior grubunun faaliyetleri, Türkiye'nin nükleer enerji santrallerine bir tehdit olarak değerlendirilmeyeceklerini göstermektedir.[98] Ancak siyasi havadaki bir değişiklik konumlarını ve davranışlarını değiştirebilir. Türk hükümetinin beklenmeyen saldırıları önlemek için grubun faaliyetlerini takip etmesi sağduyulu olacaktır.

F) Türk Güvenliği

Türk Güvenliği 2006 senesinde bilinen bir hacker ve grubun şimdiki lideri olan Agd_Scorp tarafından kurulmuştur. Türk Güvenliği fuse.microsoft.com, The Register[99] ve Vodafone'a yapılan saldırılar sonrası uluslararası olarak tanınmışlardır. *The Guardian* grubun faaliyetlerini şu şekilde tarif etmiştir:

> "*Pazar gecesi bir Türk hacker grubu aralarında the Telegraph, UPS, Betfair, Vodafone, National Geographic, bilgisayar yapımcısı Acer ve teknoloji haberleri sitesi Register'a trafiği saptırmış ve farkında olmayan kullanıcıları şifreleri, e-posta hesapları ve diğer bilgilerinin çalınması riskine sokmuşlardır."*[100]

Saldırılardan sonra *The Guardian* grupla röportaj yapmış, bu da grubun uluslararası ününü arttırmıştır.[101] Araştırma yapıldığı sürede Türk Güvenliği'nin internet sitesi faal olmamakla birlikte,

---

[97] HP Security Research, "Cyber Risk Report 2015", s.11, http://www.asial.com.au/documents/item/113 (11 Haziran 2015 tarihinde erişilmiştir)

[98] Daha fazla detay için bkz; Cyber-Warrior'un basın sözcüsü XY: Emniyet'in 5 katı iş yapıyoruz", http://psikologdoctor.blogcu.com/unlu-turk-hackerdan-muthis-aciklamalar/2454785 (7 Haziran 2015 tarihinde erişilmiştir)

[99] İngiliz menşeli ve iyi bilinen, teknoloji üzerine bir internet sitesi

[100] Charles Arthur, "Turkish hacker group diverts users away from high-profile websites", The Guardian, 05 Eylül 2011, http://www.theguardian.com/technology/2011/sep/05/turkish-hacker-group-diverts-users. (07 Haziran 2015 tarihinde erişilmiştir)

[101] Charles Arthur, "Interviewed: the Turkish hackers whose DNS attack hit the Telegraph", The Guardian, 05 Eylül 2011

Agd_Scorp'un Pastebin[102] internet sitesinde yaklaşımını kısaca netleştirdiği bir manifestosuna erişilmiştir:

> "*Uğrunda savaşman gereken şey özgürlüktür. Dünya beni tanımayabilir. Ancak yeraltında bazı kişiler benim kim olduğumu bilir ve bazıları yaptığım işleri bilir.*
>
> *Hep internette büyük kurumları hacklemeyi hayal etmiştim. Kısa bir süre sonra hayallerim gerçek oldu.*
>
> *Google, Microsoft, MSN, NATO, Nintendo, Sony, NASA, Kaspersky, Avast, AOL, Pentagon, TrendMicro, CocaCola, Peugeot, UNESCO, .mil domain'lerini, Yahoo, Playstation Network, UPS, National Geographic, Telegraph, The Register, spam.org, resellerclub.com, eNom ve hatta fbijobs.gov & interpol.com'u hackledim."*[103]

Zone-H Türk Güvenliği'nin 225 adet[104], Agd_Scorp'un da 424[105] tahrifini kaydetmiştir. Grup başlangıçta büyük oranda SQL enjeksiyon teknikleri[106] kullanmıştır ancak yeteneklerini ve yöntemlerini geliştirmiştir. Türk Güvenliği'nin ideolojisi net olmadığından hamlelerini öngörmek zordur; ancak bir durumda grup Suriye Elektronik Ordusu'nun (SEA) Türk hükümeti sitelerine yaptıkları phishing saldırılarına cevap vermiştir. SEA aynı zamanda kendi internet sitesinde bazı Türk resmi belgelerini sızdırmıştır ve Türk Güvenliği yanıt olarak SEA'nın internet sitesini hackleyerek Kur'an'dan bazı ayetleri içeren bir mesaj bırakmıştır.[107] Türk Güvenliği'nin SEA'nın internet sitesine yaptığı saldırı ve bıraktığı mesaj, milliyetçi duruşlarını kanıtlamıştır. Milliyetçi bir grup olduğundan Türk Güvenliği Türkiye'nin nükleer siber güvenliğine bir tehdit teşkil etmeyecektir.

G) PKK Hack Team

PKK Hack Team, Partiya Karkerên Kurdistanê (PKK) olarak da bilinen Kürdistan İşçi Partisi'nin bir koludur. PKK 1980'ler ve 1990'lar sürecinde yoğunlukla Kürt milliyetçisi bir hareket olmadan önce Marksist-Leninist bir örgüt olarak kurulmuştur. PKK Hack Team'in çevrimiçi faaliyetleri konusunda

---

[102] Pastebin çevrimiçi bir metin deposudur.
[103] Agd_Scorp, "Scorp's Manifesto", Pastebin, 11 Eylül 2012, http://pastebin.com/TsqZpx5H (12 Haziran 2015 tarihinde erişilmiştir)
[104] Turk Guvenligi, Zone-H, http://Zone-H.org/archive/notifier=TurkGuvenligi.info/page=1 (09 Haziran 2015 tarihinde erişilmiştir)
[105] Agd_Scorp, Zone-H, http://Zone-H.org/archive/notifier=Agd_Scorp (09 Haziran 2015 tarihinde erişilmiştir)
[106] SQL enjeksiyonu, kötü niyetli kullanıcıların SQL platform kullanan bir internet sitesine sitenin veritabanını kontrol etmek için SQL komutları enjekte ettikleri bir tekniktir.
[107] http://www.Zone-H.org/mirror/id/21545300

kısıtlı bilgi mevcuttur. Faaliyetlerine dair en eski haber, iki hackerın 2.307 devlet ve devlet dışı internet sitesini tahrif edip kendi imzalarını bıraktıkları 2006 senesine uzanmaktadır.[108] Polis PKK destekçisi hacker ekibinden iki kişiyi tutuklamıştır. 2008 senesinde PKK'lı hackerlardan birisi Türk polisi tarafından Diyarbakır'da rutin bir arama yapılırken yakalanmıştır. Polis hacker'ı taşıdığı ve çalıntı olduğu düşünülen dizüstü bilgisayar nedeniyle durdurmuş, ancak sonrasında şifrelenmiş gizli bilgiler, belgeler, pasaportlar, Poison Ivy isimli kötücül yazılım kodu ve Genelkurmay, Milli İstihbarat ve Jandarmaya ait video kayıtları bulmuştur. Hacker'ın evininin buna müteakiben aranması sonucu polis 924 CD-ROM, 57 DVD, 22 sabit disk ve iki dizüstü bilgisayar ele geçirmiştir. Soruşturma bu bilgileri PKK genel merkezine taşıyan PKK'lı kuryenin tutuklanmasıyla sonuçlanmıştır.

Soruşturma esnasında hacker, bütün bu bilgileri porno sitelerine kendi kötücül yazılımını yerleştirip, bu açıktan faydalanarak istihbarat servisi ve ordu mensuplarının bilgisayarlarına sızması sonucunda elde ettiğini itiraf etmiştir.[109] Hacker'ın becerileri ve PKK Hack Team'in örgütsel yetenekleri kolluk kuvvetlerinin dikkatini çekmiştir. 2011'de kolluk kuvvetleri PKK'lı hackerları tutuklamak amacıyla Şanlıurfa, Hakkari, Batman ve Gaziantep'te operasyonlar düzenlemiştir.

PKK Hack Team'in Zone-H internet sitesinde iki farklı kaydı vardır. Zone-H sitesine göre bir tanesinde PKK Hack Team'in 279 adet tahrif[110], diğerinde de 241 adet tahrifi vardır.[111] Haziran 2015 seçimlerinden önce Türkiye'nin doğusunda HÜDAPAR ve PKK arasında artan gerilim[112], siber uzaydaki çatışmayı da arttırmıştır.[113] Bu çatışmalar yeni bir hacker örgütünü, T.A.K.'yi (Teyrenbazên Azadiya Kurdistan – Kürdistan Özgürlük Şahinleri) ortaya çıkartmıştır.[114] Bu grup çoğunlukla Twitter

---

[108] "PKK'lı hacker'lar 2307 siteyi çökertti", *Radikal*, 27 Aralık 2006, http://www.radikal.com.tr/turkiye/pkkli_hackerlar_2307_siteyi_cokertti-801430 (29 Haziran 2015 tarihinde erişilmiştir)

[109] "Porno meraklisi istihbaratçılar PKK'nın hacker'ına çalışmışlar", *Radikal*, 27 Kasım 2008, http://www.radikal.com.tr/turkiye/porno_meraklisi_istihbaratcilar_pkknin_hackerina_calismis-910264; "PKK'lı hacker'ın pişmanlığına Yargıtay'dan onay", *Radikal*, 23 Şubat 2011, http://www.radikal.com.tr/turkiye/pkkli_hackerin_pismanligina_yargitaydan_onay-1040911 (29 Haziran 2015 tarihinde erişilmiştir)

[110] http://www.Zone-H.org/archive/notifier=pkkhackteam (21 Eylül 2015 tarihinde erişilmiştir)

[111] http://www.Zone-H.org/archive/notifier=Pkk%20Hack%20Team (21 Eylül 2015 tarihinde erişilmiştir)

[112] Türkiye Hizbullah'ı ve ortağı Hür Dava Partisi (HÜDAPAR), IŞİD'in Suriye sınırının diğer yakasındaki Kobane'yi kuşatmasına karşı Türkiye çapında 7 Ekim'de yapılan protestolar sırasında PKK ile bazı çatışmalara girmiştir. İki taraf arasındaki gecenin en kanlı çatışması Güneydoğu'daki Diyarbakır'da en azından 10 kişinin ölümüne sebep olmuştur. Daha fazla detay için bkz, Metin Gürcan, "Kurd vs. Kurd: internal clashes continue in Turkey", *AlMonitor*, 09 Ekim 2014, http://www.al-monitor.com/pulse/originals/2014/10/turkey-syria-kurds-kobani-pkk-kurdo-islamists.html# (11 Kasım 2015'te erişilmiştir) Daha fazla okumak için: http://www.al-monitor.com/pulse/originals/2014/10/turkey-syria-kurds-kobani-pkk-kurdo-islamists.html#ixzz3rZvyedSY

[113] "Hüdapar yöneticisinin hesabına hack", Özgür Gelecek, 11 Şubat 2015, http://www.ozgurgelecek.net/guncel-haberler/13494-2015-02-11-16-01-45.html (30 Haziran 2015'te erişilmiştir)

[114] https://twitter.com/tak_hacktim

hesaplarını hedef almış ve düşük bir profil sergilemiştir.[115] Özetle, tüm PKK yanlısı hacker grupları nükleer enerji tesislerine tehdit teşkil ederler. Saldırı düzenlemek için başka hacker gruplarıyla ortak çalışabilirler. Dahası, PKK ve PKK Hack Team melez kabiliyetlerini kullanarak tesislere daha fazla zarar verebilirler. Kritik altyapıyı felç etmek için hem kinetik hem de siber saldırılar kullanma becerisine sahip tek örgüttürler. Dolayısıyla hem kamunun hem de özel sektörün grubu yakından takip etmesi gereklidir.

Sonuç: Ankara'nın Geleceğe Dair Planları

Ülkenin siber güvenlik programının önümüzdeki beş yıl için bir yol haritasını çıkarmaya çalışan Kalkınma Bakanlığı, 2014-2018 için "Bilgi Toplumu Stratejisi ve Eylem Planı" isimli bir taslak plan yayınlamıştır. Planda Türkiye'nin siber güvenlik kabiliyetlerinin geliştirilmesi için beş iddialı eylem sıralanmıştır.[116] Bunlardan ilk ikisi 2015 senesinin sonunda kadar 2000'lerin başından beri tartışılan Ulusal Bilgi Güvenliği Kanunu'nun çıkarılması ve Kişisel Verilerin Korunması Mevzuatının onaylanması çağrısını yapmaktadır. Üçüncü önerilen eylem, 2016'da Siber Suçla Mücadele Stratejisi ve Eylem Planı'nın oluşturulmasıdır. Bu hedefle görevlendirilen kurumlar Emniyet Genel Müdürlüğü, Adalet Bakanlığı, İçişleri Bakanlığı, Dışişleri Bakanlığı, Jandarma Genel Komutanlığı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı[117] ve Telekomünikasyon İletişim Başkanlığı olmuştur. Dördüncü eylem internetin güvenli kullanımı konusunda en iyi uygulama kuralları konusunda farkındalığın arttırılmasıdır. Taslak belgede son olarak yer verilen eylem ise 2015 sonuna kadar bilişim suçları konusunda uzmanlaşmış mahkemelerin kurulmasıdır.

Türkiye zaman içerisinde siber uzaydaki mevcudiyetini ve kabiliyetlerini geliştirmiş olsa da, bu bütün alanlarda aynı seviyede olmamıştır; bunun neticesinde bazı alanlarda büyük aşamalar kaydedilse de diğer alanlarda beklenen ilerleme kaydedilememiştir. Diğer yandan son birkaç senede siber güvenlik ile ilgilenen devlet kurumlarının sayısı artmıştır ve Türk güvenlik güçleri siber tehditlerle mücadeleye ek bir vurgu yapmıştır. Ayrıca bazı meselelerin siyasallaştırılması Türkiye'nin siber alandaki kabiliyetlerini geliştirme arzusunu zorlaştıran bir etken olmuştur; önemli taslak yasaların çıkartılamaması ve TÜBİTAK'ta ciddi boyutta beşeri sermayenin kaybedilmesi buna örnek

[115] "PKK yandaşı hackerlar Sözcü gazetesinin twitter hesabını hackledi", *Mynethaber*, 02 Şubat 2015, http://www.mynet.com/teknoloji/pkk-yandasi-hackerlar-sozcu-gazetesinin-twitter-hesabini-hackledi-1687883-1; "PKK'lı hackerlar belediyenin hesabını hackledi", *Cumhuriyet*, 05 Şubat 2015, http://www.cumhuriyet.com.tr/haber/turkiye/207781/PKK_li_hackerler_belediyenin_hesabini_hack_ledi.html (30 Haziran 2015'te erişilmiştir)

[116] T.C. Kalkınma Bakanlığı (2014, May) "2014-2018 Bilgi Toplumu Stratejisi ve Eylem Planı (Taslak)" Aşağıdaki bağlantıdan erişilebilir: http://bilgitoplumustratejisi.org/tr/doc/8a94819842e4657b01464d5025b80002

[117] Ulaştırma, Denizcilik ve Haberleşme Bakanlığı da 2014-2018 için bir stratejik plan yayınlamıştır. Bu plan 2013-2014 Eylem Planı'nda belirlenen hedefleri tekrar teyit etmiş, ancak onların ötesine geçememiştir. Bkz. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Stratejik Planı 2014-2018

teşkil etmektedir. Bunların neticesinde Türkiye siber güvenlik alanındaki hazırlıkları itibariyle belli başlı müttefikleri ve hatta hasım devletlerin gerisinde kalmaya devam etmektedir.

Türkiye'de faaliyet gösteren hacker ve cracker grupları hakkında açık kaynak bilgi kısıtlıdır. Milliyetçi hedeflerle hareket eden grupların devlet hedeflerine saldırması pek olası değildir, hatta bunun aksine devlet karşıtı gördükleri grupları hedef aldıkları görülmüştür. Hatta Cyber Warrior (Akıncılar) gibi bazı grupların devletle doğrudan bağlantıları bile olabilir. Ancak bazı hacker gruplarının özellikle hükümet karşıtı eylemlere destek verdikleri bilinmektedir. Redhack ve PKK Hack Team gibi grupların, kendi kaynaklarıyla ya da uluslararası gruplarla işbirliği aracılığıyla, özel olarak ülkenin kritik ulusal altyapısına ve genel itibariyle Türkiye'nin siber güvenliğine ciddi sorunlar teşkil etme ihtimalleri mevcuttur.