BİLİMSEL-TEKNOLOJİK GELİŞMELERİN TERÖRİZME ETKİSİ OLARAK SİBER TERÖRİZM VE TÜRKİYE İÇİN SİBER TERÖR TEHDİDİ*

The Cyber Terrorism as the Effect of Scientific-Technological Developments on Terrorism and the Threat of the Cyber Terrorism for Turkey

Elşan İZZETGİL**

Öz

Bilimsel-teknolojik gelişmelerin imkân ve fırsatlarından iyi niyetli insanlarla birlikte teröristler gibi karanlık gündemli kişiler de faydalanmaktadır. Teröristlerin eylemlerinde teknolojileri kullanmaları yeni güvenlik sorunlarını doğurmaktadır. Siber terörizm bunlardan biri olup terörizmin sanal alana taşımasıyla ortaya çıkmıştır. Terör örgütleri, hacker gruplarının bilgi ve becerilerini edinmeleriyle birlikte eylemlerini sanal ortamda yapar duruma gelmişlerdir. Bu araştırma da terör örgütlerinin sanal alanla ilişkileri üzerine odaklanmaktadır. Çalışmada bilimsel teknolojik gelişmelerin teröristlere sağladığı olanaklar incelenmekte, internet ile terörizm arasındaki ilişki üzerinde durulmakta ve siber terörün ulaştığı düzey anlatılarak bunun Türkiye üzerindeki tehdit boyutu ele alınmaktadır.

Anahtar Kavramlar: *Bilimsel-Teknolojik Gelişmeler, İnternet, Siber Terör, Siber Güvenlik, Türkiye.*

Abstract

Along with well-intentioned people, those who have dark intentions, such as terrorists also benefit from the opportunities and facilities that the scientific and technological developments have been provided. The usage of the technologies by the terrorists in their acts creates new security problems. The cyber terrorism is one of them, and it has been emerged along with the shift of terrorism to the virtual space. The terrorist organizations who have been gained the knowledge and skills of hacker groups have come to the point of doing their acts in a virtual environment. This study focuses on the relationship of terrorist organizations with virtual space. The research explores the opportunities that have been offered by scientific-technological developments to the terrorists, focuses on the relationship between the Internet and terrorism, and discusses the level reached by cyber terrorism and its threat dimension on Turkey.

Keywords: *Scientific Technological Developments, Internet, Cyber Terrorism, Cyber Security, Turkey.*

* **Makale Geliş Tarihi:** *15.10.2021* **Yayına Kabul Tarihi:** *04.12.2021*

** Dr. Öğr. Üyesi, Kastamonu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Uluslararası İlişkiler Bölümü, e-posta: eizzetgil@kastamonu.edu.tr, ORCID: 0000-0002-8121-8348.

GİRİŞ

Bilimsel ve teknolojik gelişmelerin küreselleşmeyle yakın ilişkisi vardır. Küreselleşmenin en fazla kabul gören dönüşümcü (transformationalist) yaklaşımına göre, öneki dönemlerden farklı olarak son 40-50 yıllık süreçte teknolojideki ilerleme dünyayı küçültmüş ve insanlar arası etkileşimi artırmıştır. Özellikle Soğuk Savaş'ın son bulmasından sonra küreselleşme olgusu daha da hızlanmıştır.

Bilgisayarın icadı, internetin bulunması, mobil telefonlarının kullanıma sokulması ve mobil uygulamaların geliştirilmesi küreselleşmenin hızlanmasında çok büyük etkiye sahip olmuştur. Günümüzde en fakir insanlar bile son teknoloji ürünlere sahip olabilmekte ve yaşamlarında aktif olarak kullanmaktadırlar. Hal böyle olunca artık dünyanın herhangi bir yerinde gerçekleşen olaydan kısa zaman içinde haberdar olmak mümkün olmaktadır. Bireyler arası, toplumlar arası hızlı etkileşim olanakları doğmuştur. Bu olanaklar, fırsatların yanında riskler de yaratmıştır. Söz konusu durum, küreselleşmenin olumlu ve olumsuz dikotomilerini içinde barındırdığı ekonomik, siyasi, kültürel ve güvenlik gibi boyutlarını gündeme getirmiştir.

Devletler, artan uluslararası ticaretten pay almak için ekonomilerini küresel dünyaya eklemlemek durumda kalmışlardır. Küreselleşmenin ekonomik boyutu, toplumlar arası gelişmişlik düzeyini daha da derinleştirirken, küreselleşmenin kültürel boyutu yerel kültürlerin popüler kültür karşısında zor durumda kalmasını, gelişmiş ülke toplumsal değerlerinin yerel kültürleri ortadan kaldırma tehdidi savurduğunu göstermiştir. Küreselleşmenin siyasi boyutu ise ulus devletin sınırlarını aşındırmış, devletin toplum üzerindeki otoritesini sarsarak devlet içi kontrolsüz alanlar ortaya çıkartmıştır. Küreselleşmenin güvenlik boyutu da teknolojik gelişmelerden iyi niyetli insanların faydalanabildiği gibi kötü niyetli kişilerin de yararlanması ve insanlığa karşı tehdit oluşturmasına imkân sağladığını konu edinmiştir. Bu bağlamda insanlar üzerinde korku

salarak belli siyasi amaçlarını gerçekleştirmeye çalışan teröristler de kendileri için güvenli liman olarak gördükleri teknolojinin olanaklarını kullanmak konusunda azami çaba içerisine girmişlerdir. Özellikle de gelişmiş internet ağları ve teknolojileri teröristler için cazibe merkezi haline gelmiştir.

Teknolojik gelişmeler bir taraftan insanların daha rahat, daha huzurlu bir şekilde yaşamalarını sürdürebilecekleri olanaklar ortaya çıkarırken diğer taraftan insanlığın mahvına neden olabilecek yeni silah türlerinin icat edilmesine de neden olmaktadır. Devletler bağımsızlıklarını korumak ve güçlerini dünyaya kabul ettirmek için yeni teknolojilerin olanak sağladığı silahlara hemen sahip olmaya çalışmaktadır. Bu durum, özellikle Soğuk Savaş döneminde kitle imha silahları gibi silahların üretilmesiyle hat safhaya çıkmıştır. Korkulan ise birçok devletin sahip olduğu kitle imha silahlarını terör örgütlerinin elde etmesi veya bunları üreten tesislerin siber terör saldırısına uğramasıdır.

Yeni iletişim teknolojileri, insanlara bulundukları yerden bilgisayarının internet bağlantılarını kullanarak dünyanın öbür ucundaki bir devlete, tesise, bir şirkete veya herhangi bir bireye zarar verebilme imkânı sunmaktadır. Hatta internet bağlantısıyla kitle imha saldırılarına ulaşmanın mümkün olup olmadığı konularında araştırmalar yapılmaktadır. Bu da tehlikenin boyutları konusunda fikirler vermektedir. Teröristlerin internet üzerinden yaptıkları faaliyetleri kapsayan siber terörün, 21. yüzyılda ulusların güvenliğini çok fazla tehlikeye sokacağı artık anlaşılmış durumdadır.

Bu çalışma bilimsel teknolojik gelişmelerin gelmiş olduğu nokta itibarıyla sağladığı imkânlar dolayısıyla teröristlerin herkes gibi bunlardan istifade etmesiyle beliren tehdit boyutuna odaklanmaktadır.

Çalışmada, bilimsel teknolojik gelişmelerle ilgili bilgi verilerek, teröristlerin de kullanmak istediği ve kullanabileceği yeni silah türlerine değinilmekte, internet ve terörizm arasındaki ilişki irdelenmekte, siber terörizm ve Türkiye için siber tehdidin boyutları ele alınmaktadır.

BİLİMSEL-TEKNOLOJİK GELİŞMELER VE TERÖRİZME SUNDUĞU OLANAKLAR

Terörizmin[1] gelişim süreci incelendiğinde, teknolojik ilerlemelerle terörizmin yayılmasının aynı çizgiyi takip ettiği anlaşılmaktadır. Bu konuda Brian Jachson, teröristlerin teknolojiyi kullandıkça geliştiklerini ve daha etkili olduklarını ifade etmiştir.[2] Ulaştırma araçlarındaki teknolojik gelişmeler, terörizme her dönemde yeni olanaklar sunmuştur. Bunlardan ilki, ulaştırma araçlarının mesafeleri kısaltmasıyla teröristin kısa zamanda yer değiştirmesinin kolaylaşmasıdır. Bir ülke içinde şiddet eyleminde bulunan bir terörist, kısa zaman içinde bir başka ülkeye geçerek izini kaybettirebilmektedir. Bu durum, terörizmle mücadeleyi zorlaştırdığı gibi uluslararası nitelik kazanmasına da sebep olmaktadır.

İkinci bir olanak ise haberleşme kapsamında yaşanmaktadır. Buna Rus Çarlığı döneminde sisteme karşı halkı örgütleyen "Narodnaya Volya"nın (halkın iradesi) yöntemi örnek verilebilir. Örgüt bastığı gazetelerin hızlı şekilde yayılması ve militanlarının çabuk hareket etmesi için dönemin ileri teknolojisi sayılan telgraf ve trenleri ulaşım ve haberleşme aracı olarak kullanmıştır. Bu yöntem, örgütün Çarlık yönetimi karşısında etkili

1 Terörizm, siyasal hedeflere ulaşmak için korkutma, yıldırma, şiddet ve tehdiş kullanarak amaçlarına ulaşmaya çalışan grupların barışçıl olmayan ve demokratik nitelik taşımayan eylemleri şeklinde tanımlanmaktadır. Konu hakkında detaylı bilgi için bkz. Mehmet Seyfettin Erol, "Uluslararası İlişkiler Aktörü Olarak Terör Örgütleri", *Terörizm,* Haydar Çakmak, der., Barış Platin Yayınları, Ankara 2008, s. 73-98.

2 Michele Zanini, "The Networking of Terror in the Information Age", *Globalisation and the New Terror,* David Martin Jones, der., Edward Elgar Pub, Carolina 2004, s. 173.

olmasında en önemli etkendi.[3] Diğer bir olanak ise teröristlerin ulaşım araçlarını silah şeklinde de kullandıkları gerçeğidir.

11 Eylül 2001 tarihli terör saldırılarında da görüldüğü gibi, ulaşım aracı olan uçaklar kaçırılarak kitle imha silahına dönüştürülmüştür.[4]

Silah konusunda değinilmesi gereken bir diğer önemli konu, Soğuk Savaş dönemimde aşırı üretilen kitle imha silahlarının teröristlerin eline geçme ihtimalinin hala gerçekliğini koruyor oluşudur. Teknolojinin gelişmesiyle birlikte yeni terörizm şekilleri ortaya çıkmaktadır. Teröristler, teknolojiyi de kullanarak büyük devletlerin caydırıcılık için ürettikleri kitle imha silahlarının bilgilerini ele geçirerek bunları kendi amaçları doğrultusunda kullanmak istemişlerdir. Bu da yeni kavramların ortaya çıkmasına sebep olmuştur. "Nükleer, Biyolojik, Radyolojik ve Kimyasal Terörizm (NRBC Terörizm)" örneğinde olduğu gibi, kitle İmha Silahları, konvansiyonel (geleneksel) silahlara oranla çok daha öldürücü özelliklere sahiptir. Devletler bu silahların teröristlerin eline geçmesinden korkmaktadır.[5] Bütün zorluklara rağmen teröristlerin mevzubahis silahları kullanmaya istekli oldukları ve bunun için birçok yolu denedikleri görülmüştür.

Amerika Birleşik Devletleri'nde (ABD) 1984 yılında bir tarikat Oregon'da restoranlardaki salata barlarını bağırsak sistemini rahatsız eden bir ajanla zehirlemeyi başarmış, bunun sonucunda 751 kişi hastalanmıştır. ABD'DE 11 Eylül saldırılarından sonra yaşanan şarbonlu mektup olayları da bir diğer örnektir. Saldırılarda devlet dairelerine içinde kuru formdaki

3 Deniz Ülke Arıboğan, *Tarihin Sonundan Barışın Sonuna Terörizmi Anlamak ve Anlamlandırmak,* Timaş Yayınları, İstanbul 2003, s. 19-21.

4 N.R. Kleinfield, "U.S.Attacked; Hijacked Jets Destroy Twin Towers and Hit Pentagon in Day of Terror", *The New York Times,* 12 Eylül 2001.

5 Sovyetler Birliği dağıldığında hem ABD hem de Rusya nükleer silahların teröristlerin eline geçmesinden korkmuş ve bunun için önlemler almaya çalışmıştır. Boris Yeltsin, Bağımsız Devletler Topluluğu'nu (BDT) kuran anlaşmalara nükleer silahların kontrolünün sağlanması için madde konulmasını sağlamıştır. Bunun yanında Kazakistan'daki nükleer başlıkları kontrol altına almak için Kazakistan'la da anlaşma yapmıştır. Detaylı bilgi için bkz. Fırat Purtaş, *Rusya Federasyonu Ekseninde Bağımsız Devletler Topluluğu,* Barış Platin Yayınları, Ankara 2005, s. 65.

şarbon ajanlarının bulunduğu zarflar gönderilmiş, zarfları açan kişiye zarar vermesi sağlanmıştır. Ölümcül etkisi olan şarbon ajanı, insanlara zarar verdiği için kurumlar pek çok işlemden geçirilerek dezenfekte edilmiştir.[6]

ABD'de 1972 yılında Chicago güvenlik güçleri, sağcı-ayrılıkçı bir kişiyi yanında 35–40 kg Typoid bakterisiyle yakalamıştır. Bu kişinin soruşturulmasında bakteriyi St. Louis ve diğer batı şehirlerinde suyu zehirlemek için kullanmayı planladığı anlaşılmıştır.[7]

Teröristlerin biyolojik kimyasal silahları kullandığıyla ilgili ilk örnek ise 1995 yılında Japonya'da kayda alınmıştır. Aum Shinriyko isimli terör örgütü, Tokyo şehrinin metro istasyonlarından birinde sarin gazı kullanarak saldırı yapmıştır. Saldırıyı yapan örgütün gücü, saldırıdan çok daha fazla dikkat çekmiştir. Örgüt "M Group" isminde bir bilgisayar şirketi sıfatıyla faaliyette bulunmuş ve 2000 yılına kadar devlete ve büyük endüstri devlerine teknoloji hizmeti vermiştir. Newsweek'in 2000 yılındaki raporuna göre, teknoloji her zaman Aum terörist örgütünün gizli silahı olmuştur. Şirketin kurucuları, 1980'li yıllarda kendi çabasıyla sokak-sokak dolaşarak elektronik aletler satmaya başlamış ve daha sonra da mağazaya dönüşmüştür. 2000 yılına gelindiğinde varlıkları bir milyar Amerikan dolarına ulaşmıştır.

Konumuzla ilgili en ilginç tarafı ise grubu oluşturan Shoko Asahara'nın gıda mühendisleri, kimyacılar ve Japonya'daki prestijli üniversitelerden bilgisayar uzmanlarından oluşan bir ekiple birlikte kitle imha silahları geliştirmeye çalışmış olmasıdır.[8] Tokyo'daki metro istasyonunda cereyan eden olaylarda da tren kontrol sistemi kullanılarak sarin gazının etkili olmasını sağladıkları belirtilmiştir. Bu örnekten de anlaşılacağı gibi, varlığı milyar dolarla ölçülen bir terör örgütünün kitle imha silahlarını

6 Güler Işın, "Biyolojik Silahlar", *Pivolka,* Savaş Özel Sayısı, 2003, s. 9-11.

7 François Hant, "The Asymetric Charakter of Evolving Chemical, Biological and Nucleer (CBN) Threat", *Globalisation and the New Terror,* David Martin Jones, der., Edward Elgar Pub, North Carolina 2004, s. 121.

8 Kevin O'Brien, "Information Age Terrorism and Warfare", David Martin Jones, der., *Globalisation and the New Terror,* Edward Elgar Pub, North Carolina 2004, s. 142.

elde edebilme ve kullanabilme arzusu, duyulan endişesinin hiçte yersiz olmadığını göstermektedir.[9]

Aum örgütü ve El Kaide'nin nükleer silah elde etmek için birkaç girişimde bulundukları bilinmektedir. Aum tarikatı, 1993 yılında nükleer enerji alanında Rusya'nın önde gelen kurumlarından olan Kurçatov Enstitüsü'nden zenginleştirilmiş uranyum almayı; hatta burada çalışan hocaları kendi araştırmacı guruplarına katmayı istemiş; fakat sonuç alamamıştır. Bir defasında da Avustralya'dan Uranyum getirme teşebbüsünde bulunmuştur.[10] Bununla birlikte ABD'nin 2001 yılında Afganistan'a müdahalesinden sonra elde edilen bilgilere göre, El Kaide terör örgütü de nükleer silahları incelemiş ve bu teknolojiyi elde etmek için planlar yapmıştır.[11]

Biyolojik ve kimyasal silahların yanında "elektromanyetik bomba" olarak isimlendirilen silah da teröristlerin eline geçme ihtimali dolayısıyla ciddi tehdit kaynağı sayılmaktadır. Kısaltılmış adıyla "e-bomba", tek bir tuğlayı kırmadan ve tek bir damla kan akıtmadan tüm bir kenti yıkabileceğinden dehşet vericidir. Hazırlanması çok kolay olan bu bombayı oluşturacak mekanizmayı bir araya getirip büyük bir hasar meydana getirmek için dahi olmaya gerek görülmediği belirtilmektedir. Bu silahın sabotaj ve terörist uygulamalar için potansiyel bir silah olduğu iddia edilmektedir.[12] Göz açıp kapayana kadar uygarlığı 200 yıl öncesine götürebilecek bu silahı yapmak için ödenmesi gereken miktar yalnızca 400 Amerikan dolarıdır. İhtiyacınız olan teknoloji ise 1940'ların teknolojisidir. Bu özelliklerinden dolayı e-bomba, terörle mücadele halindeki dünyanın ciddiye alması gereken bir

9 Jones, *a.g.m,* s. 142-143.

10 Gavin Cameron, "The Biological, Radyological and Nucleer (CBRN) Threat-Exaggeretion or Apocolypse Soon?", *Globalisation and the New Terror,* David Martin Jones, der., Edward Elgar Pub, North Carolina 2004, s.102.

11 Cameron, *a.g.m,* s. 12.

12 Osman Gürdal, "Elektromanyetik Bombaların Etkileri ve Hasar Vericilikleri", *Adli Bilimler Dergisi,* 3(3), 2004, s. 57-68.

tehdittir. Halihazırda bu silah Çin, ABD, Rusya, Kuzey Kore ve İran başta olmak üzere bazı ülkeler tarafından üretilmiştir.[13]

Elektromanyetik bombanın temelini oluşturan düşünce üretilen yüksek güçte bir radyo dalgası ya da mikrodalga atımının önüne çıkan tüm elektronik devreleri yok etmesidir. Neredeyse etrafınızdaki her şeyin elektrikle çalıştığı bir çağda yaşadığımız düşünülürse, böylesi bir yöntem kitlesel bir yıkım yaratmak için korkunç bir silah olarak gözükmektedir. Bunu kullanarak taşıma sistemleri durdurulabilir, iletişim çökertilebilir ya da bilgisayar ağlarına zarar verilebilir. ABD, bu silahı 1999 yılında yürüttüğü operasyonlarda Sırpların radar sistemlerini vurmak amacıyla kullanmıştır.[14]

İNTERNET İLE TERÖRİZM ARASINDAKİ İLİŞKİ

Dünya 1970'li yıllarda Sanayi Devrimi kadar önemli bir devrim sayılan Teknoloji Devrimi'ne tanıklık etmiştir. Bu yeni devrime, "Bilişim Devrimi" de denilmektedir. Özellikle 1990 sonrasında gelişen internet, genişleyen ağı sayesinde tüm dünyayı kısa zamanda çevrelemeyi başarmıştır. İnternet, zaman mekân kavramını ortadan kaldırdığı gibi, dünyanın herhangi bir yerindeki bilgiye sadece bir tuşla ulaşmayı da mümkün kılmıştır. İnternette her türlü bilgi yayınlanmakta veya saklanabilmektedir. İnternet vasıtasıyla faydalı bilgilere erişildiği gibi topluma zararlı ve tehlikeli bilgilere de ulaşılmaktadır.

İnsanların çeşitli amaçlarla İnterneti kullandığı kabul edilirse, "düşman", "kötü" ve "kızgın" olarak tanımlanan kişilerin de interneti kullanmalarının kaçınılmaz olduğu anlaşılabilir. Kötü niyetli bu kişiler, topluma zarar vermek için yasak olan bilgilere izinsiz ulaşmak, bu bilgileri kötü niyetlerle kullanmak ve yasak olan bilgileri internette yayınlayarak insanları olumsuz yönde etkilemek gibi amaçlarla internetten istifade

13 "Rus Yapımı Elektromanyetik Süper Bomba, ABD'yi Endişelendiriyor", *Sputnik News,* https://tr.sputniknews.com/savunma/201901281037340042-rusya-elek tro manyetik-super-bomba-abd/, (Erişim Tarihi: 27.11.2020).
14 Selçuk Kılıç, "Biyolojik Silahlar ve Biyoterörizm", *Türk Hij Den Biyol Dergisi,* 63(1-2-3), 2006, s. 1-3.

edebilmektedirler. İnterneti sadece bireyler değil; organize suç örgütleri ve terör örgütleri gibi toplum için daha tehlikeli gruplar da kullanmaktadır. Bu gruplar, internet vasıtasıyla hem gelirlerini artırmakta hem de geleneksel suç türlerinin dışında yeni suç türleri ortaya çıkarmaktadırlar.

Devletlerarası ve ulusal güvenliği tehdit eden ve hedefine ulaşmada hiçbir sınır tanımayan terör örgütleri, bilgisayar teknolojisi yardımıyla tahminlerin ötesinde bir kabiliyet kazanarak uluslararası suç trafiğine yeni bir boyut kazandırmışlardır. Terör örgütleri birçok amaç için bilgisayarları kullanabilmektedir. Bir genelleme yapmak gerekirse, teröristlerin interneti beş amaç için kullandığı söylenebilir. Bunlar şöyle sıralanabilir:

- Bilgi aktarmak (saldırı dâhil);
- Finans sağlama;
- NetWork oluşturma;
- Taraftar toplama;
- Bilgi toplama

BİLGİ AKTARMA

Teröristler, bu amacı propaganda, psikolojik savaş ve bilgi transferi için kullanmaktadır. İnternet, teröristlerin yanlış enformasyon yaymak, insanları tehdit etmek ve web sitelerinde çirkin görüntüler yayınlayarak insanların üzerinde psikolojik baskı oluşturmak için kullandıkları vazgeçilmez araçtır.[15]

Aslında teröristler medyayı kullanarak eylemlerini duyurabilmekte; fakat medya sansür uyguladığı için bazen istedikleri dönütleri almaları engellenebilmektedir. Teröristler, eylemlerinin hedefe ulaşmasının

15 Maura Conway, "Terrorist 'Use' of the Internet and Fighting Back", *Cybersafety: Safety and Sequrity in a Networkked World: Balancing Cyber-Rights and Responsibilities,* Oxford Internet Instute, 8-10 Eylül 2005.

engellenmemesi için kendilerine ait internet siteleri kurarak istedikleri belge ve görüntüleri yayınlayabilmektedir.[16] Terör örgütleri bazen eylemlerini planlamak için elemanları arasında şifreli e-postalar aracılığıyla iletişim kurmakta, bazen de politik ve ideolojik anlamda bir propaganda aracı olarak interneti kullanmaktadırlar. Örnek olarak 1996 yılında Peru'nun Lima şehrinde Japonya Büyükelçiliği'ne yapılan saldırıyı verebiliriz. ABD'de ve Kanada'da sempatizanları olan Tubac Amaru adlı terör örgütü, ilgili büyükelçiliğe saldırıda bulunarak diplomatik, askeri ve siyasi personeli rehin almıştır. Birkaç ülkede bulunan örgüt üyeleri, faaliyetlerini destekleyen birçok web sitesi kurmuş ve kişileri arasındaki koordinasyonu internet üzerinden sağlamıştır. Hatta büyükelçiliğe yapılan eylemin planlarını da bu siteler vasıtasıyla paylaşmıştır.[17] Diğer bir örnek ise Meksika'da faaliyet gösteren Zapatista National Liberation Army'dir (Zapatista). Zapatistalar, 1994 yılında başlattığı ayaklanmada interneti yoğun bir propaganda faaliyeti için kullanmıştır. Kolombiya'da faaliyet gösteren The Revolutionary Armed Forces of Colombia örgütü ve Peru'daki Shining Path örgütü de interneti propaganda aracı olarak etkin şekilde kullanan diğer terör örgütleridir.[18]

ABD'nin Irak'ı işgalinden sonra terör örgütleri tarafından kaçırılan, işkence edilen ve öldürülen yüzlerce kişinin ilk olarak teşhir edildikleri yer, yine örgütlere ait internet siteleri olmuştur. Örgütler, bu sayede hem propagandalarını yapmışlar hem de toplum ve bireyleri arasında iletişim kurmuşlardır. Yine ABD'nin Irak müdahalesi sonrası oluşan siyasi boşluktan yararlanarak büyüyüp küresel bir terör örgütüne dönüşen Devletü'l Irak ve'ş Şam (DEAŞ), birçok amaç için interneti aktif şekilde kullanmıştır. Bir DEAŞ web sitesinde yazılmış "Cihad'ın yarısı medya'dır" sloganından da anlaşılacağı gibi örgüt, felsefesini pazarlamak ve bu uğurda psikolojik savaş uygulamak için yazılı görsel basını silah gibi kullanmıştır. Bunu da

16 Cindy C. Combs, *Terrorism in the Twenty-First Century,* Prentice Hall, New Jersey 2003, s. 151.
17 Combs, *a.g.e,* s. 151-152.
18 *Aynı yer.*

birçok dilde yayın yapan, çeşitli web sayfaları, sosyal medya hesapları, oyunlar ve çizgi filim uygulamaları aracılışıyla yürütmüştür.[19]

DEAŞ "siber cihat" adı altında birçok siber saldırı gerçekleştirmiştir. DEAŞ'ın saldırılarına birçok ülke maruz kalmıştır. En fazla saldırı ise ABD, Avrupa, İsrail, İran ve Türkiye'ye karşı düzenlenmiştir. Amerikan Merkez Kuvvetler Komutanlığı (CENTCOM) resmi Twitter ve Youtube hesapları, 2015 yılında "Siber Halife" lakaplı Birminghamlı Junaid Hussein (Ebu Hüseyin El Britani) tarafından hacklanmıştır. Hesaplardan "Amerikan askerleri arkanızı kollayın, kişisel telefonlarınızı ve ailelerinizi biliyoruz" mesajı yayınlayarak örgütün propagandasını yapılmıştır.[20] DEAŞ'ın güçlü olduğu 2014-2016 yıllarında ABD'deki valilere ve yayın kuruluşlarına ait hesaplar ele geçirilmiş ve buralardan da ABD Başkanı Barack Obama ve ailesine yönelik tehdit mesajları yayınlanmıştır.

Donald Tramp döneminde ise Tramp'a yönelik "İslam devletini seviyorum. Donald Trump, Müslüman ülkelerde akıtılan her damla kan için hesap verecektir" gibi mesajlar yayınlanmıştır.[21] 9 Nisan 2015 tarihinde "Siber Halife" lakaplı terör örgütü mensubu kişi(ler) Fransa'nın TV5 Monde (200'den fazla ülkeye yayın yapan ve bünyesinde 11 televizyon bulunan kanal) kanalının yayınını keserek buradan mesaj yayınlamıştır. Mesajda "Hollande, haksız bir savaşa katılarak affedilmez bir hata yaptın. Bu nedenle Parisliler, Ocak'ta Charlie Hebdo ve Kosher Süpermarket hediyelerini aldılar." denilmiştir.[22]

19 Sertaç Canalp Korkmaz, *Terörün Propagandası: DAEŞ Terör Örgütü ve 'Konstantiniyye' Dergisi,* ORSAM, 2016, s. 7.

20 Mehmet Halil Mustafa Bektaş-Ali Yasin Gündoğdu, "IŞİD'in Hibrit Savaş Stratejileri: Hibrit Savaş Konsepti Perspektifinden Analizi", *International Journal of Politics and Security,* 1(1), 2019, s. 49.

21 "V SŞA khakeri razmestili propagandu İGİL na pravitelstvehhıkh saytakh" (В США хакеры разместили пропаганду ИГИЛ на правительственных сайтах), *NW,* https://n-w.tv/v-ssha-khakery-razmestili-propagandu-ig/, (Erişim Tarihi: 08.12.2020).

22 "İslamskoye gosudarstvo" ustroilo noç koşmara dlya franstuzkikh" («Исла́мское госуда́рство» устроило ночь кошмара для французских), *NTV,* https:/ /www.ntv.ru/novosti/1391081, (Erişim Tarihi: 08.12.2020).

Özetle terör örgütlerinin interneti propaganda aracı olarak kullanmaları genel bir durum arz etmektedir. Özellikle küresel terör örgütü olarak bilinen DEAŞ'ın interneti bütün amaçları için ve maharetle kullanmış olduğu görülmektedir. Hatta DEAŞ'ın küresel bir örgüt haline gelmesi bağlamında gücünü internetten aldığını ifade etmek yanlış olmayacaktır.

FİNANS SAĞLAMA

Terör örgütlerinin faaliyetlerini sürdürebilmeleri ve ayakta kalabilmeleri finansal durumlarına bağlıdır. Teröristler, bağışçı bulmak veya illegal yollardan para temin etmek için kendilerinin ya da başkalarının kurdukları siteleri aktif şekilde kullanmaktadırlar. Teröristler, kendi sitelerini ziyaret eden kişilerin vicdan ve duygularıyla oynayarak onlardan para temin edebilmektedir.[23] Lübnan da bulunan İran yanlısı Hizbullah, internet üzerinden kitap ve diğer yayınlarını satarak mali destek sağlamaktadır.[24]

İnternet üzerinden finans sağlama kapsamında DEAŞ terör örgütünden de bahsetmek gerekmektedir. DEAŞ web siteleri üzerinden hesap numaralarını yayınlayarak dışarıdan bağışlar toplamıştır. Bunun yanında yeni teknoloji sayılan sanal para birimi Bitcoin sisteminden yoğun şekilde faydalanmıştır. Yine Hawala[25] sistemini de para aktarmalarında kullanmıştır.[26] Bunlara internet kullanıcılarının kredi kartı bilgilerinin boşaltılarak elde edildiği paraları ve internet dolandırıcılığı gibi yöntemleri de eklemek mümkündür.

NETWORK OLUŞTURULMASI

Teröristler, NetWork'u kullanarak dünyanın neresinde olurlarsa olsunlar birbirleriyle iletişim sağlayabilmektedir. Zira teröristler, daha fazla

23 Conway, *a.g.m.*

24 Mehmet Özcan, "Yeni Milenyumda Yeni Tehdit: Siber Terör", *Türk Harb-İş Dergisi,* 210, 2004, s. 39.

25 "Hawala" yasa dışı olarak toplanan paraların başka küresel finans sistemine takılmadan bir ülkeye illegal yollarla transfer edilmesi anlamına gelmektedir. Detaylı bilgi için bkz. Bektaş-Gündoğdu, *a.g.m.,* s. 48.

26 Bektaş-Gündoğdu, *a.g.m.,* s. 49.

güçlenebilmeleri için kendi ülkeleri dışındaki milletlerle iletişim kurmaya ihtiyaç duymaktadır. Hem farklı terör örgütlerinin liderleri hem de kendi örgütlerindeki kişilerin birbiriyle iletişim sağlamalarında internet en başta gelen vazgeçilmez araç olarak kabul edilmektedir. 11 Eylül saldırısıyla suçlanmış teröristlerin sorgulamasında öğrenildiğine göre, e-posta yoluyla haberleşmeyi tercih etmişlerdir. Aynı şekilde 2002'de Oregon'da yakalanan 4 kişi, e-posta kullanarak Afganistan'daki terörist örgütlerle bağlantı kurdukları ve onlara yardım ettikleri, kendilerinin de bu ülkeye giderek ABD'ye karşı mücadele etmeyi planladıkları için suçlanmışlardır.[27] Burada verdiğimiz iki örnekte de e-postanın kullanılmasının sebebi internetle cep telefonları karşılaştırıldığında, internetin daha güvenli görülmesidir.

TARAFTAR TOPLAMAK (ANGAJE ETMEK)

Teröristler, örgütleri içerisinde görmek istedikleri kişileri yanlarına çekmek için de interneti kullanmaktadırlar. Yaygın kullanılan "chat" türünde konuşma uygulamalarını kişilerle tanışmak için kullandıkları ve kişiler hakkında genel bilgi edindikten sonra bunları daha geniş sorgulama için sadece kendi militanlarının bulunduğu başka uygulamalara yönlendirdikleri bilinmektedir. Burada eğer kişiler istedikleri kalitede ise onlarla canlı olarak tanışmakta ve içlerine dâhil etmektedirler. Bu şekilde güvenlik endişesine kapılmadan karşılarındaki adayları eleme şansı bulmaktadırlar.[28]

DEAŞ terör örgütünün militan toplama "başarısı" burada örnek gösterilebilir. DEAŞ, 2014 senesinde el-Kaide'nin bu örgütle bağlarını kestiğini ilan etmesiyle birlikte bağımsız hareket etmeye başlamıştır. Örgüt, kısa zaman içinde rekor sayıda militan toplayarak Irak ve Suriye topraklarının büyük bir kısmını kontrol altına almayı başarmıştır.

Londra merkezli Siyasi Şiddeti Araştırma Merkezine dayandırılan bir bilgiye göre, 2013 yılının Aralık ayında Suriye ve Irak'ta 74 ülkeden 11 bin militan DEAŞ'a katılmıştır.

27 Conway, *a.g.m.*
28 Conway, *a.g.m.*

Merkezi Haberalma Teşkilatı'nın (CIA) 2014 yılının Eylül ayı raporlarına göre, bu rakam 31 bine ulaşmış, 2016 yılı Ocak ayı itibarıyla ise Irak'ta 50 bin, Suriye'de 30 bin olmak üzere toplam 80 bin (15 bin yabancı) militanın DEAŞ saflarında savaşa katılmasında internet belirleyici olmuştur.[29]

BİLGİ TOPLAMA

Sanal depolama yöntemleri gelişmeden önce, bilgi belli yerlerde dokümanlarda tutulmaktaydı. Ancak günümüzde fiziki yer sorunu ve hızlı erişim gerekçeleriyle bilgiler, sanal ortamda depolanmakta ve hatta eski bilgi ve belgelerde taratılarak sanal ortama aktarılmaktadır. Bundan dolayı internette istenilen bilgiye en kısa zamanda ulaşmak mümkün hale gelmiştir. İnternet, teröristler için de bilgi edinmenin kolay, ucuz ve tehlikesiz yolu haline gelmiştir. 2003 yılının Ocak ayında yaptığı bir konuşmada dönemin ABD Savunma Bakanı Donald Ramsfeld şu ifadeye yer vermiştir:[30]

> *"…Bizim sitemizde birçok gizli olmayan materyal vardır ve bunu teröristler kendi amaçları için kullanabilirler. Bakanlığın sitesinde, bakanlığın planları, programları ve faaliyetleri hakkında 700 GB'den fazla bilgi bulunmaktadır. Ayrıca sitede nükleer reaktörlerin nerede oldukları hakkında bilgi vardır. Biz hiç unutmamalıyız ki, düşmanlarımız siteyi her zaman ziyaret edebilir. 11 Eylül olaylarından sonra teröristlerin kullanabilecekleri bilgi devlet sitelerinden alınmıştır. Nükleer komisyon hemen kendi bilgilerini yayından çekmiştir."*

29 Elşan İzzetgil, "Orta Asya ve Kafkasya'da Köktendinci Hareketler ve IŞİD Tehdidi", *Türk Dünyası 25 Yıllığı,* Mehmet Seyfettin Erol-Yavuz Gürler, der., Akçağ Yayınları, Ankara 2016, s. 83-84; Jim Sciutto vd., "ISIS Can 'Muster' between 20,000 and 31,500 Fighters, CIA Says", *CNN,* https://edition.cnn.com/2014/09 /11/world / meast/isis-syria-iraq/index.html, (Erişim Tarihi: 05.12.2020).

30 Conway, *a.g.m.*

Teröristler, elemanlarını ve sempatizanlarını eğitmek amacıyla interneti yoğun olarak kullanmaktadırlar. Terör örgütleri, web sayfalarında "Teröristin El Kitabı", "Teröristin Yemek Kitabı" gibi kaynakları yayınlamaktadır. Bu kitaplarda bomba yapımı en ince detaylarıyla anlatıldığı gibi, bir teröristin bilmesi gereken birçok konuda ayrıntılı bilgiler de yer almaktadır.[31]

Güvenlik güçleri, siyasiler ve diğerleri bombanın yapılışıyla ilgili bilgilerin sitelerde yer almasından endişe duymaktadır. Bu konuda en hassas ülkelerin başında ABD gelmektedir. Öyle ki; 1997 yılının Nisan ayında ABD Adalet Bakanlığı, bu tür bilgilerin internette yer almasının teröristlerin ve hukuka karşı olanların işini kolaylaştırdığı açıklamasında bulunmuştur.[32]

Konuya ilişkin Maura Conway, Jessca Stern isimli bir kimyacının Türkçe tercümesiyle "Bakteri Savaşı: Kuzey Amerika'daki Tehdit" isimli 1995 senesinde yayınlanmış eserini örnek vermektedir. Bu eserde bir alt başlıkta bakteri üretimi ve çoğaltılmasıyla ilgili geniş bilgi verildiğine dikkat çekerek söz konusu kitabın hem birkaç internet sitesinde yayınlandığını hem de kitapçılarda 13 Amerikan doları gibi uygun bir fiyattan satıldığını söyleyerek, bu bilgilerin teröristlerin ellerine geçmesinin mümkün olabileceğinin altını çizmiştir.[33]

El Kaide, Hizb-ut-Tahrir, İslami Cihat ve hatta Hamas örgütlerinin, militanlarına internet üzerinden haritalar, fotoğraflar ve bomba yapımında kullanılan teknik bilgileri ayrıntılı bir şekilde paylaştıkları bilinmektedir.[34]

İnsanlar, teröristlerin kullanabileceği silahların yapımıyla ilgili bilgilerin internette yayınlanmasının engellenmesini istemektedir. Fakat internetin tam olarak kontrol edilememesi yüzünden hem imkânsız

31 "Terrorist Activities on the Internet", *ADL*, http://www.adl.org/Terror/focus/ 16focus _a.asp, (Erişim tarihi 09.01.2011); "PKK'nın El Kitabı Ortaya Çıktı", *Sabah,* https://www.sabah.com.tr/gundem/2018/10/09/pkknin-el-kitabi-ortaya-cikti, (Erişim Tarihi 27.11.2020).

32 Conway, *a.g.m.*

33 Conway, *a.g.m.*

34 Brien, *a.g.m.,* s.143; Zanini, *a.g.m.,* s.172.

olarak gözükmekte hem de teröristlerin aynı bilgileri başka yerlerden yine temin edebilecekleri gerçeğini ortadan kaldırmamaktadır. Burada Jessica Stern'in 1982 yılında kimyasal maddelerle yapılan deneyler ile ilgili yayınlanmış bir başka kitabını örnek gösterebiliriz. Bahse konu olan kitabın sınırlı sayıda yayınlanmış olmasına rağmen teröristlerin bunu bulmalarının imkânsız olmadığını ve hatta bu tür yayınların farmakolojik dergilerde de yayınlandığını söylemek mümkündür.[35]

SİBER TERÖRİZM VE TEHDİT BOYUTU

Terörizm tanımı konusunda fikir birliği olmadığı gibi siber terörizm konusunda da genel kabul görmüş bir tanım yoktur. Siber terörizm tanımı konusunda en önemli sıkıntı "hacker" saldırıları ile siber terör arasında farkın tam olarak ortaya konulmamış olmasıdır. İngiltere'nin 2000 yılında kabul ettiği terör yasasında siber terörizm, "hükümeti etkilemek ya da toplumu korkutmak amacıyla elektronik sistemlerin içine izinsiz girmek veya bu sistemleri bozmak" şeklinde tanımlanmıştır. Bu yasaya bakıldığında, bir grup internet eylemcisi herhangi bir devlet memurunun resmi e-posta adresine, e-posta protestosu gerçekleştirir ve bu e-posta sisteminde bir çöküntüye neden olursa, bunun siber terörizm olarak değerlendirileceği sonucunu çıkarmak mümkündür. Dolayısıyla yasa, bilgisayar korsanlarını da siber terörizm tanımı kapsamında göstermektedir.[36]

Diğer taraftan Amerikalı bilgisayar bilimi profesörü Dorothy Denning'in tanımında siber terörizm daha dar tutulmuştur. Bu tanım şöyledir: [37]

> *"Siber terörizm, belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin*

35 Conway, *a.g.m.*

36 Özcan, *a.g.m.,* s. 39; Jenkins, *a.g.m.,* s.13.

37 Dorothy Denning'nin konuyla ilgili görüşleri hakkında detaylı bilgi için bkz. "Cybersecurity's Next Phase: Cyber-Deterrence", *The Conversation,* https://theconversation.com/cybersecuritys-next-phase-cyber-deterrence-67090, (Erişim Tarihi: 27.11.2020).

bireylere ve mallara karşı; bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır."

Bir başka tanım da şu şekilde yapılmıştır: [38]

"Siber boşluk ile terörizmin bir birleşimi olarak siber terörizm, siyasi ve sosyal mercilere ve kişilere gözdağı vermek, baskı oluşturmak maksadıyla resmi birimlerin bilgisayarlarına, network sistemlerine, bilgi ve veri tabanlarına yapılan yasadışı tehdit ve zarar verici saldırılardır. Ancak bir saldırının siber terörizm olarak tanımlanabilmesi için bir bireye ve mala karşı şiddet içermesi gerekmektedir."

Diğer bir önem verilmesi gereken tanım ise Desouza ve Hensgen'nın yaptığı tanımdır:[39]

"Bilgi sistemleri doğrultusunda, elektronik araçların, bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla, ulusal denge ve çıkarların tahrip edilmesini amaçlayan, kişisel ve politik olarak motive olmuş, amaçlı eylem ve etkinliklerdir."

Bahsi geçen tanımların "hacker" saldırılarını siber terörizmden ayırt etmek için yapıldığı açıkça anlaşılmakta; fakat "hacker" saldırılarının "şiddet" kapsamında ele alınması gerektiğini ifade eden uzmanların sayısının hayli fazla olduğu düşünülürse, siber terörist eylemleri hacker eylemlerinden ayırt etmek için elimizde tek özellik kalmaktadır. Bu da politik motiftir. Bu durumda herhangi bir politik motiften hareketle planlanmış olan ve dijital ortamda gerçekleştirilen bilgi toplama ya da zarar verme amaçlı saldırı eylemini siber terörizm olarak tanımlamak mevcut koşullarda mümkündür.

38 Denning, *a.g.m.*

39 Desouza, Kevin C.-Tobin Hensgen, "Semiotic Emergent Framework to Address the Reality of Cyberterrorism", *Technological Forecasting and Social Change,* 70(4), 2003, s. 385-396.

Yapılan tanımlardan da yola çıkarak klasik terör ile siber terör arasında bazı farklılıkların olduğu anlaşılmaktadır. Bu farkları birkaç başlık altında toplamak mümkündür.

FİZİKSEL RİSK FARKI

Klasik anlamda terör eyleminde bulunan teröristin ölme riski çok yüksektir. Silahlı ve bombalı olarak katıldığı eylemde güvenlik güçleri tarafından etkisiz hale getirilebilir. Lakin dünyanın herhangi bir yerinde, bilgisayarının başında oturarak internet üzerinden hedefine aldığı bir devlete, bir topluma, zararı ve tehdit boyutu açısından normal bir terörist eylem kadar olan, büyük ses getirecek saldırıda bulunabilir. Bu eylem, onun yaşamını herhangi bir şekilde tehlikeye sokmayacaktır.

AMAÇ FARKI

Terörün asıl amacı politiktir, yapılan şiddet eylemleri ise bu amaca ve hedefe ulaşmak için bir araçtır. Politik amaçları gerçekleştirmek için bilişim yöntemlerinin kullanılması söz konusudur. 2008 yılında Rusya ile Gürcistan arasında yaşanan savaş esnasında Rusya tarafından Gürcistan'a yapılan siber taarruzda ülkedeki neredeyse tüm web sayfaları, finans merkezleri, haberleşme sistemleri ve elektrik santraller işlemez hale gelmiştir.

Söz konusu saldırı hem Gürcistan halkını hem de dünya kamuoyunu psikolojik olarak etki altına almak ve sonuç olarak da Gürcistan Hükümeti'nin siyasi olarak zor durumda kalmasını sağlamak amacıyla yapılmıştır.[40]

FİZİKSEL ETKİ FARKI

40 Kerim Göztepe-Ahmet Ejder, "Siber Terör Saldırılarından Korunmaya Yönelik Bulanık Mantık Tabanlı Karar Destek Modeli", *Siber Güvenlik Çalıştayı,* Ankara 2011, s. 2.

Klasik terör, belli sayıdaki teröristin yine belirli noktalarda yaptığı eylemleri kapsamaktadır. Teröristler olabildiği kadar geniş ses getirmek isterler ama yaptıkları eylemin ve mekânın belli bir çapı, genişliği ve adresi vardır. Herhangi bir sembolik bina hedef alınmışsa, o bina çökebilir ve içindeki şahıslar yaşamlarını yitirebilir. Ancak siber terörde eylemin direk fiziki etki alanı, bilgisayarı yönlendiren kişinin elinin altındaki fareye bir tıklama hareketiyle inanılmaz şekilde genişletilebilir. Bir tıklamayla devlete/devletlere ait binlerce internet sitesi aynı anda çökertilebilir. Yani birden çok eylem aynı anda gerçekleştirilebilir.

Wikileaks adlı site buna örnek verilebilir. Karanlık ilişkilerinin de olduğu anlaşılan Julian Assange adlı bir internet aktivistinin başında olduğu bir grup, ABD'li büyükelçilerin ve önemli diplomatlarının görevli oldukları ülkelerle ilgili edindikleri ve merkeze gönderdikleri gizli bilgileri ele geçirmiş ve web sitelerinde yayınlamıştır. Bu durum, ülkeler arasında birtakım sorunlara neden olurken; ABD'li diplomatlara güvenilemeyeceği fikri oluşmuştur.[41]

PSİKOLOJİK ETKİ FARKI

Siber terörün insanları etkileme gücü; bilgisayar ve bilgi teknolojisi, internet bağlantısının genişliği ve güvenlik önlemlerinin sağlamlığıyla ilgilidir. Çünkü siber saldırı, bilgisayar üzerinden yapılmakta, hedeftekiler ise bilgisayar ve bilgisayar teknolojisi kullanan kişiler olmaktadır. Fakat günümüzde artık bilgisayarın girmediği yer hemen-hemen hiç kalmamıştır. Artık hizmetler, bilgisayar üzerinden verilmektedir. Bundan dolayı gerekli hizmetlere ulaşamamanın insanlarda oluşturacağı bunalımın etkisi yıkıcı olabilmektedir.[42] Özellikle genç nesiller, bilgisayara bağımlı halde yetişmektedir. Litvanya'daki siber saldırıda da görüldüğü gibi, neredeyse

41 "WikiLeaks.org Is Dead; Long Live WikiLeaks.ch", *NBR,* https:// www.nbr.co.nz/article/wikileaks-offline-faces-triple-threat-134238, (Erişim Tarihi: 27.11.2020).

42 Denning, *a.g.m.* s. 70.

ülkedeki bütün hizmetler verilemez duruma gelmiştir. İnsanlar belirsiz süre, hiçbir şey yapamadan hizmet almak için beklemek zorunda kalmıştır.

Klasik teröre göre siber terörün insanlar üzerinde fiziki etkisi belki az olabilir. Zira klasik terörde yaralanmalar ve ölümler olabilmektedir. Lakin siber terörün tesirinin yayılma alanının geniş olması, insanlar üzerinde çok önemli psikolojik hasarlar bırakmaktadır.[43]

KİŞİ GÜVENLİĞİ FARKI

Geleneksel terörde kişinin güvenliğini tehdit edecek eylem sıklığı, güvenlik birimlerinin fiziksel önlemleri artırmasıyla hafifletilmektedir. Siber terörde ise kişi; eylemin hızı ve kolaylığı nedeniyle daha fazla tehdit altındadır.

YAŞ FARKI

Terör örgütlerinin fiziki güç kullanımı söz konusu olduğunda elemanlarını en azından belirli bir yaşın üzerindeki kişilerden seçmektedir. Ancak siber terörde çocuk denecek yaştaki insanlar terörün aracı haline gelebilir. Zira macera arayan ortaokul ve lise öğrencileri eylemlere karışabilmektedir. Özellikle de ABD'de Pentagon'un veya diğer devlet birimlerinin web siteleri hedef seçilmektedir.

Bilgisayar kullanım yaşı ile silah kullanım yaşı arasında bir karşılaştırma yapıldığında, bilgisayar kullanımının çok küçük yaşlarda başladığı görülmektedir.[44] Bundan dolayı siber terör suçlarında yaş ortalaması da düşmektedir.

43 Ali Burak Darıcılı, "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıları Analizi", *U.Ü. Sosyal Bilimler Enstitüsü Dergisi,* 7(2), 2014, s. 1-10.

44 Haydar Çakmak-Taner Altunok, *Suç Terör ve Savaş Üçgeninde Siber Dünya,* Barış Platin Kitabevi, Ankara 2009, s. 40-50.

KULLANILAN SİLAH FARKI

Son olarak siber teröristler klasik teröristler gibi eylemlerini gerçekleştirmek için bomba veya silahlara değil; bir bilgisayar ve modeme gereksinim duymaktadır.[45] Bu sayede hem eylemlerini çok daha kolay bir şekilde gerçekleştirebilmekte hem de güvenlik güçlerine yakalanma risklerini minimuma indirmektedirler.

Terör örgütleri, daha güvenli buldukları bir alan olan internete hızlı bir şekilde taşınmaktadırlar. Teröristler, propaganda yapma konusunda sanal alanı ustalıkla kullanmaktadır. Finans sağlama ve para aktarma konularında da interneti kullanmayı tercih ettikleri söylenebilir. Şiddet konusunda da her geçen gün yeteneklerini geliştirdikleri görülmektedir.

27 Nisan 2007 tarihinde Estonya'nın başkenti Tallin'deki Kızıl Ordu Anıtı'nın kaldırılması üzerine bu ülkeye ait önemli web siteleri Rus hackerlerin saldırısına uğramıştır. Estonya Hükümeti, devlet kurumlarıyla birçok özel işletmenin internet sitelerini çökerten bu saldırıdan Moskova'yı sorumlu tutmuştur. Bunun üzerine iki ülke ilişkilerinde gerginlikler yaşanmıştır.

İnternetin çok yaygın olarak kullanıldığı bu ülkede iki hafta boyunca önemli devlet ve banka hizmetleri verilemez duruma gelmiştir.[46] Estonya Cumhurbaşkanlığı, parlamento, bakanlıklar, siyasi partiler ve bankalarla birçok önemli işletmenin internet siteleri hedef alınmış, aşırı yüklenme nedeniyle ana işlemcileri çökmüş ve ülkenin dış dünyayla bağlantısı kesilme noktasına gelmiştir.[47]

45 Özcan, *a.g.m.,* s. 38.

46 "Estonya'ya Siber Saldırı" *BBC Turkish,* http://www.bbc.co.uk/turkish/news/story /2007/05/070517_estonia_cyber.shtml, (Erişim Tarihi: 13.12.2020).

47 "İlk Siber Savaş", *Habertürk,* https://www.haberturk.com/dunya/haber/23642-ilk-siber-savas, (Erişim Tarihi: 13.12.2020).

Estonya yönetiminin daveti üzerine AB ve NATO, Siber Terörizmle Mücadele Birimi (NCSA) uzmanlarını acil olarak Tallin'e göndermiştir.[48]

Uzmanlar söz konusu ülkeye siber güvenlik tedbirleri almada yardımcı olmuştur. Estonya'yla birlikte Litvanya'da Rus hakerlerin yoğun saldırısına uğramıştır. Bu saldırı hasebiyle Litvanya'dan yapılan açıklamada, dış güçlerin siber saldırılarından bahsedilmiştir. Bahse konu olan siber saldırılardan sonuç çıkaran 7 NATO üyesi (Estonya, Letonya, Litvanya, İtalya, Almanya, İspanya ve Slovakya), 14 Mayıs 2014 tarihinde imzaladıkları anlaşmayla Estonya'da konuşlanacak bir ortak siber savunma merkezi kurulması konusunda işbirliği yapma kararı almıştır.[49]

Dünya'nın özellikle de teknolojiyi yoğun olarak kullanan devletlerin asıl korktukları şey, teröristlerin siber alanı bir silah gibi kullanma ihtimalidir. 2000'lerin ortalarında yapılan araştırmalarda, yapılan öngörülerde, ileride olması muhtemel terör aktiviteleri şu şekilde sıralamıştır:[50]

- Şehirlerin bütün altyapı hizmetleri sekteye uğratılabilir.
- Acil yardım faaliyetleri, hastaneler ve itfaiyenin çalışması engellenebilir.
- İletişim ağları kapatılabilir.
- Telekomünikasyon hizmetleri durdurulabilir.
- Elektrik ve doğalgaz arzu kesilebilir.
- Ulaştırma ve su sistemleri karmaşıklaştırılabilir.
- Bankalar ve finans sektörü çökertilebilir.

48 Bilal, Karabulut, "Uluslararası İlişkilerde Savaş Olgusunun Yaşadığı Dönüşüm: Hibrit Savaş ve Rusya Örneği", *Karadeniz Araştırmaları,* 15(55), 2017, s. 127.

49 "Siber Savaşta Cepheler Şekilleniyor", *Wordpress,* https://uzmannet.wordpress.com/2008/07/24/siber-savasta-cepheler-sekilleniyor/, (Erişim Tarihi: 13.12.2020).

50 Gamze Helvacıköylü, "Siber Terörizm Nedir", *TASAM,* https://tasam.org/tr-TR/Icerik/515/teror_nedir, (Erişim Tarihi: 13.12.2020).

- Bilgisayar sistemleri karmaşık hale getirilebilir.
- Hükümet kurumları ve güvenlik birimleri alt üst edilerek sistem birden durdurulabilir ve tahmin edilemeyen birçok hizmet aksatılabilir.

Yukarıda bahsedilen öngörülerin üzerinden çok geçmeden Estonya ve Litvanya'ya siber saldırı gerçekleşmiş, sıralanan ihtimallerin birçoğu yaşanmıştır. Beklide uzmanlar bu öngörülerde bulunurken olayların bu kadar hızlı ve yakın tarihte hayata geçeceğini tahmin etmemişlerdir. Bu da tehlikenin düşünüldüğünden daha hızlı bir şekilde insanlığı kuşatmaya başladığını göstermektedir.

Siber tehdidin ne kadar büyük olduğunu göstermek için şu örneği verilebilir: Birleşik Devletler Ulusal Güvenlik Ajansı (NSA), 1997 yılında "Eligible Recieved" (Uygun Alıcı) kod adlı bir tatbikat gerçekleştirmiştir. Tatbikat kapsamında bilgisayar hackerlerinden müteşekkil 35 adet "kırmızı takım" oluşturulmuş ve onlardan belirli kurallar çerçevesinde ulusal güvenlik sistemlerini karıştırmaları istenmiştir. Hawaii'deki Pasifik Komutanlığı ise tanımlanmış ilk hedef olarak seçilmiştir. Bu tatbikatta, takım üyelerinin sadece bilgisayar yazılımlarını ve internetten kolayca elde edilebilen hacker araçlarını kullanmalarına izin verilmiştir. Tatbikatın sonucu dehşet verici olmuştur. "Kırmızı Takım" internet üzerinde herkese açık olan hacker araçlarını kullanarak Pasifik bölgesindeki bütün Amerikan askeri komuta sistemlerine zarar verilebileceğini göstermiştir.[51]

Tatbikatın sonucunun bu derece korkunç ve hackerler için kolay bir görev olmuş olması, ilerleyen dönemlerde teröristlerin siber alanı daha etkili kullanacaklarının işareti sayılmıştır. Hazırlanmış bir raporda, teröristler tarafından barajların kapaklarının açıldığını, doğalgaz basıncının artırıldığını, trafik lambalarının kapatıldığını, ilaç üreten bir laboratuvarın

51 "Siber Terörizm", *TASAM,* https://tasam.org/Files/Icerik/File/siber_terorizm_ raporu_84be5753-d219-418f-9a68-e6c719b645b1.pdf, (Erişim Tarihi: 13.12.2020).

bilgisayarına sızıp ilaçlara katılan maddelerin gramajlarıyla oynandığını ve yukarıda belirtilen olasılıkların birkaç tanesinin birden gerçekleştirildiğini düşünmemiz istenmiş ve bu durumun devletler için hüsran olabileceği ifade edilmiştir.

Olası bir saldırının gerçekleşmemesi için siber alanın güvenliğinin sağlanmasına milyar dolarlarca yatırım yapılmaktadır. En çok terör tehdidiyle karşı karşıya olan ABD, 11 Eylül saldırılarından sonra siber terörle mücadele için 30 milyar dolar bütçe ayırmıştır.[52] ABD'de teknolojik suçlar ve siber terörizmle mücadele eden pek çok yapı ve bu kuruluşlara ait özel birimler oluşturulmuştur. Bunlardan bazıları şunlardır: FBI National Inftastructure Protection Center, Information Technology Association of America, Trap and Trace Center Authority ile Carnegie Mellon's Emergency Response Team. Bunların dışında bazı üniversitelerin bünyesinde de çeşitli birimler kurulmuştur.

1996 yılının Temmuz ayında Commission of Critical Infrastructure Protection (Kritik Altyapılar Koruma Komisyonu) adlı ABD Başkanı'na bağlı bir komisyon oluşturulmuştur. Bu komisyon, elektronik haberleşme ve bilgisayar ağlarının ABD açısından hayati önem taşıdığını, söz konusu ağların dış saldırılara açık ve kamu ve özel sektörün mevcut tehditleri ciddiye almadığını belirterek bu ağların korunması için önlemler alınması gerektiğini savunmuştur.[53] Görüldüğü gibi ne kadar önlem alınırsa alınsın siber saldırılar, tehdit olarak varlığını korumaktadır. Yukarıdaki örneklerden de anlaşıldığı gibi birkaç yıl önce uzmanların uyardıkları alanlara bugün saldırılar yapılmaktadır.

Teröristlerin siber alanı bu kadar yoğun kullanmaları ve hızlı uyum sağlamalarının sebebi irdelendiğinde, bilgiye kolay erişim cevabına

52 Michael Rühle, "On Yıl Sonra NATO: Ders Alıyoruz", *NATO,* https:// www.nato.int/docu/review/tr/articles/2011/09/02/on-yil-sonra-nato-ders-aliyoruz /index.html, (Erişim Tarihi: 13.12.2020).

53 "Siber Terörizm", *TASAM,* https://tasam.org/Files/Icerik/File/siber_terorizm_ raporu_84be5753-d219-418f-9a68-e6c719b645b1.pdf, (Erişim Tarihi: 13.12.2020).

ulaşılmaktadır. Batı ülkelerinde nerdeyse bütün bilgiler internette saklanmaktadır. Bu durum, devletin toplumuna hizmetini kolaylaştırmakta ve ülkeleri saldırıya da açık hale getirmektedir. Birleşik Krallık Savunma Bakanlığı'nın değerlendirmesine göre teknoloji, savaş kazanma konusunda avantaj sağladığı için yüksek teknolojiye bağımlılık artmaktadır. Mevzubahis durum, düşmanlar için de geçerlidir. Düşmanlar, askeri kabiliyetlerden dolayı aradaki güç farkını ortadan kaldırma arzusuyla alternatif yöntemlerle karşılık vermeyi tercih etmektedirler.[54] ABD Yüksek Savunma Eleştirmeni Chales J. Dunlap şunları söylemiştir:[55]

> *"Gelecekteki rakip, düşman asimetrik metotları kullanarak birleşik devletlerin hizmetlerinin durdurulmasına sebep olabilir; Bizim emirlerimizi, kontrolümüzü, iletişimimizi, istihbarat ağlarını aksatabilir veya beklediğimizden daha fazla kayba uğratabilir. Bunun içinde ulusal çözüm yolları denenmesi gerekir."*

11 Eylül 2001 tarihli terör saldırısı, o tarihe kadar birtakım resmi internet sitelerini çökertmeyle sınırlı kalan siber terörizmin hangi boyutlara ulaşabileceğini gösteren bir milat olmuştur. Söz konusu saldırılarla ilgili ortaya atılan komplo teorileri bir kenara bırakılırsa, Pentagon'un kırılmaz denilen güvenlik şifrelerinin kırılması, hava radar sistemlerinin devre dışı bırakılması, düşen uçakların pilotlarından kaçırılma sinyalleri alınmaması gibi unsurlar üst üste geldiğinde, bunların en azından teknolojiden yoğun biçimde faydalanılan saldırılar olduğu anlaşılmaktadır.

Bahse konu olan terör eyleminin bir siber saldırı olup olmadığı konusunda bilim adamlarının tartışmaları devam etmektedir. Lakin bu saldırıda teknolojinin yoğun bir şekilde kullanıldığı açıktır. Bu anlamda 11 Eylül, siber teröristler için de bir cesaret kaynağı olmuştur. Estonya ve Litvanya'ya yapılan siber saldırılarda da görüldüğü gibi, teröristler artık

54 O'Brein, *a.g.m,* s.142-144
55 O'Brein, *a.g.m,* s.144

daha güvenli buldukları interneti tercih etmektedirler. Hatta Estonya devlet yetkililerinin iddiaları kanıtlanabilirse, artık siber terörün yeni boyutu, "devlet destekli siber terör" olgusu olarak ortaya çıkmaktadır.

SİBER TERÖR TEHDİDİ VE TÜRKİYE

Türkiye, tarih boyunca birçok kötü niyetli örgütle mücadele etmiş ve günümüzde de terör örgütleriyle mücadele etmektedir. Bunların başında 1980'li yıllardan itibaren özellikle de güney bölgelerde bölücü/ayrılıkçı amaçlarla faaliyette bulunan terör örgütü Partiya Karkerên Kurdistanê/ Kürdistan İşçi Partisi (PKK) gelmektedir. Türkiye'yi hedef almış bir diğer terör örgütü ise küresel terör örgütü DEAŞ'dır.

PKK propaganda yapmak için interneti oldukça yoğun şekilde kullanmaktadır. Bu örgüt veya yandaşlarının kurdukları ve yurt dışındaki serverler üzerinden yayın yaptıkları televizyon ve radyolar, geniş kitlelere hitap etmektedir.[56] PKK ve sempatizanlarının sosyal medyayı da propaganda için yoğun şekilde kullandıkları bilinmektedir. Türk polisi, sosyal medyada PKK propagandası yapan teröristleri açığa çıkararak yakalamakta;[57] fakat yurt dışında özellikle de Avrupa'da faaliyette bulunan grupları engelleme konusunda zorlanmaktadır. Teröristlerin faaliyette bulunduğu ülkelerle yapılmış anlaşmalara rağmen işbirliğinden bu devletlerin kaçınmaları nedeniyle polislerin işi zorlaşmaktadır.

Terör örgütleri sanal alanı daha etkili kullanmak için doğrudan örgüt adına faaliyette bulunan hacker grupları da oluşturmuştur. "PKK Hack Team" bunlardan biridir. "PKK Hack Team"in varlığı, 2006 yılında kayda geçen faaliyetleriyle anlaşılmıştır. Bu hacker grubu, 2006 senesinde

56 "PKK Propagandası Yapan 5 TV Kanalı", *Milliyet,* https://www.milliyet.com.tr/ gundem/pkk-propagandasi-yapan-5-tv-kanali-1574306, (Erişim Tarihi: 13.12.2020); "PKK'nın Medya Ayağına Darbe", *Sabah,* https://www.sabah.com.tr/gundem /2016/02/20/pkknin-medya-ayagina-darbe, (Erişim Tarihi: 13.12.2020).

57 "Sosyal Medyada Terör Örgütü PKK Propagandası Yapan 10 Kişiye Gözaltı", *Hürriyet,* https://www.hurriyet.com.tr/gundem/son-dakika-sosyal-medyada-teror-orgutu-pkk-propagandasi-yapan-10-kisiye-gozalti-41673442, (Erişim Tarihi: 13.12. 2020).

2307 devlet ve devlet dışı internet sitesini tahrif ederek kendi mesajlarını yayınlamıştır.

Grubun mensuplarından biri 2008 yılında Diyarbakır'da çalıntı bilgisayar şüphesiyle polis tarafından arama yapılırken yakalanmış ve kişide şifrelenmiş gizli belgeler, pasaportlar, "Poison Ivy" isimli kötücül yazılım kodu ve Genelkurmay, Milli İstihbarat Teşkilatı (MİT) ve Jandarma'ya ait video kayıtlar bulunmuştur. Kişinin evinde yapılan aramalarda ise içerisinde gizli bilgilerin bulunduğu 924 CD-ROM, 57 DVD, 22 sabit disk ve 2 bilgisayar ele geçirilmiştir. Soruşturmada hacker, söz konusu bilgileri "Poison Ivy" kötücül yazılımını porno sitelerine yerleştirip, bazı açıklardan yararlanarak istihbarat servisi ve ordu mensuplarının bilgisayarlarına sızarak elde ettiğini itiraf etmiştir. Kişinin verdiği bilgiyle bu bilgileri PKK merkezine taşıyan kurye de yakalanmıştır.[58]

Terör örgütü PKK'nın diğer hacker grubu ise "Mezopotamia Hackers" ismiyle faaliyette bulunan yapılanmadır. Ankara Emniyet Müdürlüğü İstihbarat ve Terörle Mücadele (TEM) şube müdürlükleri ile Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı, PKK içerisinde faaliyet yürüten bilgisayar korsanlarını terör örgütünün sözde kongre kararları doğrultusunda "Mezopotamia Hackers" çatısı altında birleştiğini tespit etmiştir.

1 Ekim 2020 tarihinde Ankara Cumhuriyet Başsavcılığı'nca başlatılan operasyonda terör örgütü PKK adına siber saldırılar vasıtasıyla örgüt propagandası yaptıkları tespit edilen 21 kişiye gözaltı kararı verilmiştir. Emniyetten yapılan açıklamada, şüphelilerin 81 ilde 411 kamu kurum ve kuruluşu ile 14 bin 271 tüzel kişiliğe ait internet sitelerine yönelik yetkisiz erişimler gerçekleştirerek, propagandasını yaptıkları örgüt adına

58 Salih Bıçakçı vd., "Türkiye'de Siber Güvenlik", *Türkiye'de Siber Güvenlik ve Nükleer Enerji,* EDAM, 2016, s. 58-59.

maddi taleplerde bulundukları belirtilmiştir.[59] 6 Kasım 2020 tarihinde "Mezopotamia Hackers" mensuplarına yönelik 8 ilde eş zamanlı operasyon yapılmıştır. Yakalanan teröristler çok sayıda kamu kurumu ve özel internet sitesini kırdıklarını itiraf etmişlerdir.[60]

PKK'nın muhtemel tehdit boyutuyla ilgili yapılan bir araştırmada, örgüte ait veya onun güdümünde kurulmuş hacker guruplarının Türkiye'nin ileride hizmete girecek nükleer santrallerine tehdit oluşturma potansiyelinin olduğunu iddia edilmiştir. Bununla birlikte kritik altyapıyı felç etmek için hem kinetik hem de siber saldırılar kullanma becerisine sahip oldukları için de oldukça tehlikeli bulunmuşlardır.[61]

Türkiye'ye karşı mücadele içinde olan diğer bir terör örgütü olan DEAŞ da sanal âlemi oldukça yoğun kullanabilmektedir. DEAŞ, medyadan özellikle de internet medyasından yoğun şekilde faydalanmıştır. DEAŞ Türk toplumuna ulaşmak için "Konstantiniyye" isimli elektronik dergi de çıkarmıştır. Örgüt, Türkçe konuşan ve Türkiye dışında yaşayan ve İslamofobi baskılarına maruz kalan kişileri kendi safına çekmek için bahsi geçen dergiyi propaganda aracı olarak kullanmıştır.[62] Yayına başladığı 2015 yılından 2020 yılının Aralık ayına kadar altı sayı çıkarmıştır.

Görüldüğü üzere DEAŞ, Türkiye'den militan toplamak (Türkiye'den 2100 civarında militan toplamıştır), finans sağlamak, Türkiye'deki mensuplarıyla iletişim kurmak için interneti, sosyal medyayı, mobil uygulamaları kullanmayı tercih etmiştir.[63] DEAŞ'ın Türkiye'deki ilk ciddi siber saldırısı Kamu Hastaneleri Birliği internet sitelerine yapmış ve ele geçirilmiş sitelerde örgütü öven mesajlar yayınlamıştır. Örgüt, Türk Ordusu'nun

59 "PKK'nın Siber Yapılanmasına Operasyon: 21 Gözaltı Kararı", *NTV,* https://www. ntv.com.tr/turkiye/pkknin-siber-yapilanmasina-operasyon-21-gozalti-karari,SYK4b 2zBUkOxoEX2AFrK4g, (Erişim Tarihi: 13.12.2020).

60 "Terör Örgütü PKK'nın "Hacker"larına Operasyon", *TRT Haber,* https://www.trthaber.com/haber/turkiye/teror-orgutu-pkknin-hackerlarina-operasyon-528620.html, (Erişim Tarihi: 13.12.2020).

61 Bıçakçı vd., *a.g.m.,* s. 59.

62 Korkmaz, *a.g.e.,* s.7.

63 Ceyhun Kaan Karakaş, "DAEŞ Propagandasında Yeni Medya Kullanımı", *Marmara İletişim Dergisi,* 28, 2017, s. 33-46.

kendisine yönelik operasyonları sürdürmesi halinde devlet sitelerine ve bankalara siber saldırı düzenleyeceğini açıklamıştır.[64]

DEAŞ'ın "Siber Hilafet" grubu, Türkiye'de birçok heckleme olayına kalkışmış, örgüte finans sağlamak için Türkiye'de faaliyette bulunan büyük bankaların VIP müşterilerinin banka hesaplarını ele geçirmeye çalışmıştır.[65]

Yukarıda verilen örnekler, Türkiye'ye yönelik terör odaklı siber saldırıların sadece bir kısmını yansıtmaktadır. Türkiye hem siber terör hem de genel olarak sanal saldırılarla mücadele etmek için dünyayla paralel bir şekilde önlemler almaya çalışmaktadır. Bununla ilgili ilk yapılan işler ise hukuki mevzuat üretilmesi ve yabancı ülkelerle siber güvenlikle ilgili işbirliği anlaşmaları imzalanması olmuştur.

Türkiye Dışişleri Bakanlığı aracılığıyla Almanya, Belçika ve Hollanda gibi ülkelere müracaat edilerek Türkiye aleyhine faaliyet gösteren zararlı sitelerin kapatılması için yazılar gönderilmiş; fakat olumlu yanıtların alınması ya uzun sürmüş ya da herhangi bir yanıt alınamamıştır.[66] Bu konuda Avrupa'da da mevzuat eksiklikleri mevcuttur.

Mevzuat üretilmesiyle ilgili bu zamana kadar birçok düzenleme yapılmış olduğunu belirtmek gerekmektedir. 23 Kasım 2001 tarihinde Avrupa Konseyi Siber Suçlarla Mücadele Sözleşmesi'ni imzaya açmıştır.[67] Bunun mevcut boşluğu doldurmaya yönelik ilk çalışmalardan biri olduğunu söyleyebiliriz. Türkiye, 2010 yılında bu anlaşmayı imzalamıştır.[68] Türkiye, siber suçlara yönelik ilk düzenlemesine "Bilişim Alanında Suçlar" kanun

64 Bektaş-Gündoğdu, *a.g.m.,* s. 49.

65 "IŞİD'in Türkiye'deki 'Siber Hilafet' Planı", *Al-Monitor,* https://www.al-monitor. com/pulse/tr/originals/2016/07/turkey-syria-isis-cyber-space-turkish-content.html, (Erişim Tarihi: 14.12.2020).

66 "IŞID'in Türkiye'deki…", *a.g.m.,* s. 42.

67 Yasemin Kurt, "Avrupa Siber Suçlarla Mücadele Sözleşmesi ve Türk Hukuk Mevzuatındaki Eksiklikleri", *İMEF,* http://www.imef.org.tr/Internet-Hukuku/256-Avrupa-Siber-Suclarla-Mucadele-Sozlesmesi-ve-Turk-Hukuk-Mevzuatindaki-ksiklikler.html, (Erişim Tarihi: 14.12.2020); "Terörle Mücadele Kanunu No:2713", *Resmi Gazete,* Kabul tarihi: 12.04.1991.

68 "Siber Suç Sözleşmesi [Turkish]", *OSCE POLIS,* https://polis.osce.org, (Erişim Tarihi: 14.12.2020).

düzenlemesiyle başlamıştır. Diğer önemli bir düzenleme ise 4 Mayıs 2007 tarihinde kabul edilmiş 5651 sayılı, "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"dur.[69]

Türkiye siber terörle mücadele etmek için güvenliğini her geçen gün daha fazla sağlamlaştırmaya çalışmaktadır. Milli Güvenlik Kurulu'nun (MGK) 2010 yılının Ekim ayındaki toplantısında Milli Güvenlik Siyaset Belgesi'nde köklü değişiklikler yapılmış, ulusal güvenlik için tehdit oluşturan yeni unsurlar belgeye eklenmiştir. Belgeye giren yeni tehditlerden biri de siber terördür. Yapılan açıklamada internetin ve bilgisayarın yaygınlaşması nedeniyle küresel ölçekte gündeme gelen siber tehditlerin ulusal güvenliğe tehdit olarak görüldüğü belirtilmiştir.[70]

Türkiye'de siber alanın güvenliğinin sağlanmasıyla ilgili daha ciddi önlemler ise 2010 yılı sonrasında alınmaya başlanmıştır. 20 Ekim 2012 tarih, 28447 sayılı Resmi Gazete'de yayınlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planlarını hazırlamak ve koordinasyonunu sağlama görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na verilmiştir. Bu konuyla ilgili Siber Güvenlik Kurulu da oluşturulmuştur. Siber Güvenlik Kurulu'nun 21Aralık 2012 tarihli toplantısında Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" kabul edilmiş ve Bakanlar Kurulu'nun 20 Haziran 2013 tarihli ve 28683 sayılı kararı ile Resmi Gazetede yayımlanmıştır.[71]

Söz konusu belge gelişen bilgi ve iletişim teknolojileri, artan güvenlik gereksinimi ve edinilen tecrübeler doğrultusunda Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından güncellenmektedir. 2015 yılında yapılan

69 Kurt, *a.g.m.*

70 Aydın Hasan-Murat Pazarbaşı, "Siber Tehditle Milli Mücadele", *Milliyet,* 28 Ekim 2010.

71 "Siber Güvenlik Stratejisi ve Eylem Planı", *Bilgi Teknolojileri Kurumu,* https://www.btk.gov.tr/siber-guvenlik-stratejisi-ve-eylem-plani, (Erişim Tarihi: 11.12.2020).

çalışmalarla "2016-2019 Ulusal Siber Güvenlik Stratejisi" ve "2016-2019 Ulusal Siber Güvenlik Eylem Planı" hazırlanmış ve "2020-2021 Ulusal Siber Güvenlik Stratejisi" adı altında güncellemeleri yapılmaktadır.[72] Aralıklarla güncellenen bu belgelere bakıldığında, siber alanın güvenliğinin bir bütün olarak ele alındığı anlaşılmaktadır. Hacker saldırıları, siber terör veya siber savaş gibi saldırılar benzer yöntem ve araçları kullanıyor olmaları sebebiyle bunlarla toptan mücadele edilmesi öngörülmüştür.

Türkiye'nin karşılaştığı siber terör ve siber saldırılar dolayısıyla uygulamalar yapacak kadrolarını oluşturmak için de hızlı davrandığı söylenebilir. Siber saldırılara karşı koymak için Emniyet Genel Müdürlüğü (EGM), MİT, Türk Silahlı Kuvvetleri (TSK) ve diğer kurumlar bünyesinde siber suçlarla mücadele birimleri teşkil edilmiştir. Bununla birlikte 2013-2014 Eylem Planı'nın bir getirisi olarak Siber Olaylara Müdahale Merkezi oluşturulmuştur. Telekomünikasyon İletişim Başkanlığı'nın (TİB) denetimi altında "ülkemizi etkileyebilecek tehditlere karşı 7/24 müdahale esasına göre çalışan "Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM)" ve USOM'un koordinasyonunda çalışacak sektör bazlı "Siber Olaylara Müdahale Ekipleri (SOME)" tesis edilmiştir. 2015 yılının Ocak ayı itibarıyla 720 personelle işletilen 245 kurumsal SOME teşkil edilmiştir.[73]

Ayrıca siber alanda korunması gereken bankacılık ve finans, ulaştırma, enerji, kritik kamu hizmetleri, su yönetimi ve elektronik haberleşmeden oluşan 6 adet kritik sektör belirlenmiştir. Yapılan saldırılar analiz edilerek endüstri üretimin muhafaza edilmesine karar verilmiş olduğu için Endüstriyel Kontrol Sistemleri Siber Olaylara Müdahale Timleri (EKS–SOME) teşkil edilmiştir. Siber Güvenlik Kurulu'nun kurulmasıyla birlikte TSK bünyesinde Muhabere ve Elektronik Bilgi Sistemleri (MEBS) Destek Komutanlığı oluşturulmuştur. 2012 yılının Haziran ayında ise TSK Siber

72 "2016-2019 Ulusal Siber Güvenlik Stratejisi", *Ulaştırma Altyapı Bakanlığı,* https:// www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, (Erişim Tarihi: 12.12.2020).
73 Bıçakçı vd., *a.g.m.,* s. 35-36.

Savunma Merkezi Başkanlığı'nın TSK-SSMB kurulması gerçekleşmiştir.[74] Daha sonra da 2013 senesinin Ağustos ayında TSK-SSMB ve MEBS, Siber Savunma Komutanlığı olarak bu kurum yeniden düzenlenmiştir. Siber Güvenlik Komutanlığı'nın personel sayısı 80'e çıkartılmıştır. EGM de yapılanmasını 2013 yılında oluşturmuştur. EGM Bilişim Suçlarıyla Mücadele Daire Başkanlığı, Siber Suçlarla Mücadele Daire Başkanlığı şeklinde tesis edilmiştir.[75]

SONUÇ

Siber terör, devletler ve toplumlar için yeni tür tehdit olarak belirmiştir. Artık ulusal güvenliği sağlamak için Çin Seddi gibi duvarlar, savaş uçakları ve füzeler yetersiz kalmaktadır. Gelişen teknolojilerle birlikte bilgisayarlar kullanılarak devletlerin ve toplumların ulusal çıkarları tehdit edilebilmektedir. Günümüzde en sade bireyden örgütlere ve devletlere kadar çok geniş kitle, bilgisayarı kendi çıkarları için kullanarak karşısındakilere zarar verebilmektedir.

Terör örgütleri, siyasi hedefleri doğrultusunda faaliyette bulunurken daha güvenilir buldukları sanal ortamı, olabildiğince geniş şekilde kullanmaktadırlar. Terör örgütleri, sanal ortamı daha güçlü kullanabilmek için hacker gruplarının bilgi birikimlerinden istifade etmeyi de ihmal etmemiş ve kendi hacker gruplarını oluşturmuştur. Özellikle de küresel terör örgütü olan DEAŞ, "Siber Halife" ismini kullanan grubu kurmuştur. Söz konusu grup, DEAŞ adına saldırılar düzenlemiş, ele geçirdiği sitelerde örgüt propagandası yapmış ve örgüt için finans sağlamaya çalışmıştır. Bu örgüt Türkiye'deki kurumlara da saldırılar düzenlemiştir. Türkiye'yi sanal alanda hedef alan diğer terör örgütü ise PKK'dır. PKK, bilgi toplamak ve propaganda yapmak adına "Mezopotamia Hackers" ve "PKK Hack Team" gibi grupları kurarak bunlardan istifade etmiştir. Yapılan araştırmalar, bu

74 Bıçakçı vd., *a.g.m.*, s. 36.
75 *Aynı yer.*

grupların ileride kullanıma girecek nükleer tesisler için tehdit oluşturma potansiyeli barındırdıkları yönündedir.

Kötü niyetli bireylerin sanal alanı ülkelerin stratejik altyapısını, elektrik santrallerini, hastane otomasyonlarını, bankacılık sistemini hedef alabileceğini göstermektedir. Terör örgütlerinin oluşturdukları siber grupların yaptığı faaliyetlerden ve 2008 yılındaki Gürcistan-Rusya savaşında Gürcistan'a yönelik saldırılardan ve yine Litvanya'ya yönelik siber saldırıdan bunu anlamak mümkündür.

Ülkeler, karşılaştıkları siber saldırıları aşabilmek için silahlı kuvvetler, emniyet, istihbarat ve diğer birimlerinde ekipler kurmaya ve karşı saldırıda bulunabilmek için yöntemler geliştirmeye çalışmaktadır.

Devlet mekanizmalarında işlerin ağır ilerlemesi söz konusu olduğu için daha dinamik bir anlayış gerekmektedir. Zira siber saldırılar, endişe verici durum teşkil etmektedir. Nükleer tesisler gibi stratejik yapılara telafi edilemeyecek boyuttaki bir saldırı gerçekleştirilirse, bunun yıkımı çok büyük olacaktır. Dolayısıyla siber güvenlik birimlerinin kötü niyetli insanlar ve gruplardan her zaman bir adım önde olacak şekilde örgütlenmeleri ve proaktif çalışmaları gerekmektedir.

KAYNAKÇA

"IŞİD'in Türkiye'deki 'Siber Hilafet' Planı", *Al-Monitor,* https:// www.al-monitor.com/pulse/tr/originals/2016/07/turkey-syria-isis-cyber-space-turkish-content.html, (Erişim Tarihi: 14.12.2020).

"İlk Siber Savaş", *Habertürk,* https://www.haberturk.com/dunya/haber/23642-ilk-siber-savas, (Erişim Tarihi: 13.12.2020).

"İslamskoe gosudarstvo' ustroilo noç koşmara dlya frantsuzkikh (Исламское государство» устроило ночь кошмара для французских)", *NTV,* https://www.ntv.ru/novosti/1391 081, (Erişim Tarihi: 08.12.2020).

"PKK Propagandası Yapan 5 TV Kanalı", *Milliyet,* https:// www.milliyet.com.tr/gundem/pkk-propagandasi-yapan-5-tv-kanali-1574306, (Erişim Tarihi:13.12.2020).

"PKK'nın El Kitabı Ortaya Çıktı", *Sabah*, https://www.sabah.com.tr /gundem/2018/10/09/pkknin-el-kitabi-ortaya-cikti, (Erişim Tarihi: 27.11.2020).

"PKK'nın Medya Ayağına Darbe", *Sabah,* https://www. sabah.com.tr/gundem/2016/02/20/pkknin-medya-ayagina-darbe, (Erişim Tarihi: 13.12.2020).

"PKK'nın Siber Yapılanmasına Operasyon: 21 Gözaltı Kararı", *NTV,* https://www.ntv.com.tr/turkiye/pkknin-siber-yapilanmasina-operasyon -21-gozalti-karari,SYK4b2zBUkOxoEX2AFrK4g, (Erişim Tarihi: 13.12.2020).

"Rus Yapımı Elektromanyetik Süper Bomba, ABD'yi Endişelendiriyor", *Sputnik News,* https://tr.sputniknews.com/savunma/20190128103734 0042-rusya-elektromanyetik-super-bomba-abd/, (Erişim Tarihi: 27.11.2020).

"Siber Güvenlik Stratejisi ve Eylem Planı", *Bilgi Teknolojileri Kurumu,* https://www.btk.gov.tr/siber-guvenlik-stratejisi-ve-eylem-plani, (Erişim Tarihi: 11.12.2020).

"Siber Savaşta Cepheler Şekilleniyor", *Wordpress,* https://uzmannet.wordpress.com/2008/07/24/siber-savasta-cepheler-sekilleniyor/, (Erişim Tarihi: 13.12.2020).

"Siber Suç Sözleşmesi [Turkish]", *OSCE POLIS,* https://polis.osce. org, (Erişim Tarihi: 14.12.2020).

"Sosyal Medyada Terör Örgütü PKK Propagandası Yapan 10 Kişiye Gözaltı", *Hürriyet,* https://www.hurriyet.com.tr/gundem/son-dakika-sosyal-medyada-teror-orgutu-pkk-propagandasi-yapan-10-kisiye-gozalti-41673442, (Erişim Tarihi: 13.12.2020).

"Terör Örgütü PKK'nın "Hacker"larına Operasyon", *TRT Haber,* https://www.trthaber.com/haber/turkiye/teror-orgutu-pkknin-hackerlarina-operasyon-528620.html, (Erişim Tarihi: 13.12.2020).

"Terörle Mücadele Kanunu No:2713", *Resmi Gazete,* 12.04.1991.

"Terrorist Activities on the Internet", *ADL,* http://www.adl.org/Terror/focus/16_focus_a.asp, (Erişim Tarihi: 09.12.2020).

"Ulusal Siber Güvenlik Stratejisi 2016-2019", *Ulaştırma ve Altyapı Bakanlığı,* https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, (Erişim Tarihi: 12.12.2020).

"V SŞA khakerı razmectili propagandu İGİL na pravitelctvennıkh saytakh" (В США хакеры разместили пропаганду ИГИЛ на правительственных сайтах), *NW,* https://n-w.tv/v-ssha-khakery-razmestili-propagandu-ig/, (Erişim Tarihi: 08.12.2020).

ARIBOĞAN, Deniz Ülke, *Tarihin Sonundan Barışın Sonuna Terörizmi Anlamak ve Anlamlandırmak,* Timaş Yayınları, İstanbul 2003.

BEKTAŞ, M. Halil Mustafa-Ali Yasin Gündoğdu, "IŞİD'in Hibrit Savaş Stratejileri: Hibrit Savaş Konsepti Perspektifinden Analizi", *International Journal of Politics and Security,* 1(1), 2019, s. 25-56.

BIÇAKÇI, Salih vd., "Türkiye'de Siber Güvenlik", *Türkiye'de Siber Güvenlik ve Nükleer Enerji,* EDAM, İstanbul 2016, s. 28-74.

CAMERON, Gavin, "The Biological, Radyological and Nucleer (CBRN) Threat-Exaggeretion or Apocolypse Soon?", *Globalisation and the New Terror,* David Martin Jones, der., Edward Elgar Pub, North Carolina 2004, s. 88-119.

COMBS, Cindy C., *Terrorism in the Twenty-First Century,* Prentice Hall, New Jersey 2003.

CONWAY, Maura, "Terrorist 'Use' of the Internet and Fighting Back", *Cybersafety: Safety and Sequrity in a Networkked World: Balancing Cyber-Rights and Responsibilities,* Oxford Internet Instute, 8-10 Eylül, 2005.

ÇAKMAK, Haydar-Taner Altunok, *Suç Terör ve Savaş Üçgeninde Siber Dünya,* Barış Platin Kitabevi, Ankara 2009.

DARICALI, Ali Burak, "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıları Analizi", *U.Ü. Sosyal Bilimler Enstitüsü Dergisi,* 7(2), 2014, s. 1-16.

DESOUZA, Kevin C.-Tobin Hensgen, "Semiotic Emergent Framework to Address the Reality of Cyberterrorism", *Technological Forecasting and Social Change,* 70(4), 2003, s. 385-396,

EROL, Mehmet Seyfettin, "Uluslararası İlişkiler Aktörü Olarak Terör Örgütleri", *Terörizm,* Haydar Çakmak, der., Barış Platin Yayınları, Ankara 2008, s. 73-98.

GÖZTEPE, Kerim-Ahmet Ejder, "Siber Terör Saldırılarından Korunmaya Yönelik Bulanık Mantık Tabanlı Karar Destek Modeli", *Siber Güvenlik Çalıştayı,* Ankara 2011, s. 1-7.

GÜRDAL, Osman "Elektromanyetik Bombaların Etkileri ve Hasar Vericilikleri", *Adli Bilimler Dergisi,* 3(3), 2004, s. 57-68.

HANT, François, "The Asymetric Charakter of Evolving Chemical, Biological and Nucleer (CBN) Threat", *Globalisation and the New Terror,* David Martin Jones der., Edward Elgar Pub, North Carolina 2004, s.119-127.

HASAN Aydın-Murat Pazarbaşı, "Siber Tehditle Milli Mücadele", *Milliyet Gazetesi,* 28 Ekim 2010.

HELVACIKÖYLÜ, Gamze, "Siber Terörizm Nedir", *TASAM,* https://tasam.org/tr-TR/Icerik/515/teror_nedir, (Erişim Tarihi: 13.12.2020).

IŞIN, Güler, "Biyolojik Silahlar", *Pivolka,* Savaş Özel Sayısı, 2003, s. 6–11.

İZZETGİL, Elşan, "Orta Asya ve Kafkasya'da Köktendinci Hareketler ve IŞİD Tehdidi" *Türk Dünyası 25 Yıllığı,* Mehmet Seyfettin Erol-Yavuz Gürler, der., Akçağ Yayınları, Ankara 2016, s. 83-97.

JENKINS, Brian M., "İnternational Terrorizm: A New Mode of Conflict", *İnternational Terrorizm and World Seccurity,* D.Carlton-C. Schaerf, der., Londra 1975, s. 9-15.

KARABULUT, Bilal, "Uluslararası İlişkilerde Savaş Olgusunun Yaşadığı Dönüşüm: Hibrit Savaş ve Rusya Örneği", *Karadeniz Araştırmaları,* 15(55), 2017, s.115-130.

KARAKAŞ, Ceyhun Kaan, "DAEŞ Propagandasında Yeni Medya Kullanımı", *Marmara İletişim Dergisi,* 28, 2017, s.33-46.

KLENFIELD, N. R., "U.S.Attacked; Hijacked Jets Destroy Twin Towers and Hit Pentagon in Day of Terror", *The New York Times,* 12 Eylül 2001.

KORKMAZ, Sertaç Canalp, *Terörün Propagandası: DAEŞ Terör Örgütü ve 'Konstantiniyye Dergisi',* ORSAM, 204, 2016.

KURT, Yasemin, "Avrupa Siber Suçlarla Mücadele Sözleşmesi ve Türk Hukuk Mevzuatındaki Eksiklikleri", *İMEF,* http://www.imef. org.tr/ (Erişim Tarihi: 10.01.2020).

O'BRIEN, Kevin A., "Information Age terrorism and Warfare", *Globalisation and the New Terror,* David Martin Jones, der., Edward Elgar Pub, North Carolina 2004, s.127-159.

ÖZCAN, Mehmet, "Yeni Milenyumda Yeni Tehdit: Siber Terör" *Türk Harb-İş Dergisi,* 210, 2004, s.25-40.

PURTAŞ, Fırat, *Rusya Federasyonu Ekseninde Bağımsız Devletler Topluluğu,* Barış Platin Yayınları, Ankara 2005.

RÜHLE, Michael "On yıl Sonra NATO: Ders Alıyoruz", *NATO*, https://www.nato.int/docu/review/tr/articles/2011/09/02/on-yil-sonra-nato-ders-aliyoruz/index.html, (Erişim Tarihi: 13.12.2020).

SCIUTTO, Jim vd., "ISIS Can 'Muster' between 20,000 and 31,500 Fghters, CIA Says", *CNN,* https://edition.cnn.com/2014/09/11/world/ meast/isis-syria-iraq/index.html, (Erişim Tarihi: 05.12.2020).

SEMİZOĞLU, İbrahim, "Siber Terörizm ve Biyolojik Silahlar", *Kriminal Polis Laboratuvarları,* http://www.kpl.gov.tr, (Erişim Tarihi: 08.12.2020).

ZANINI, Michele, "The Networking of Terror in the Information Age", *Globalisation and the New Terror,* David Martin Jones, der., Edward Elgar Pub, 2004, s. 159-185.

STRUCTURED ABSTRACT

Just as well-intentioned people benefit from the opportunities offered by scientific-technological development, those who have dark intentions also utilize it for their purposes. It is necessary to include the terrorists in such a group of people as well. Considering the history of terrorism, it is understood that they are trying to realize their goals, by utilizing the possibilities offered by science and technology to the maximum extent. One hundred years ago, in Russia "Narodnaya Volya" used rail transport and telegraph to provide communication and transportation since they were fast and reliable. Today, terrorists can influence millions of people from their hideouts by using cyberspace. From the early 2000s, while analyzing the terrorist organizations and terrorist incidents, which are concerned with international politics and Turkey, it is evident that organizations such as al-Qaeda, Islamic State of Iraq and Syria (ISIS/Daesh), Partiya Karkerên Kurdistanê/Koma Civakên Kurdistan (PKK/KCK) have used cyberspace quite widely and extensively. Particularly, they form groups such as the "Cyber Khalifat" of ISIS, the "Mezapotomya Hackers" of PKK/KCK, and "PKK Hacker Team", and via these groups, they attack the strategic institutions and infrastructures of the country.

The PKK/KCK uses the Internet widely and extensively to make propaganda. These organizations or their sympathizers can reach a broad audience via television and radios, which they have established, and by broadcasting over servers abroad. Furthermore, it is known that they use social media extensively for their propaganda as well. Although the Turkish police try catching the terrorists who conduct propaganda of the PKK/KCK on social media; however, they face difficulties in terms of preventing those who are active, especially in Europe. Despite the agreements made with the countries of origin in which the terrorists are active, the duties of the police have become more difficult since the contracting parties avoid cooperation.

In order to use the virtual space more effectively, terror organizations have also created hacker groups that can be active and operate directly on their behalf. “PKK Hack Team” is one of them. The existence of this terrorist group was revealed via its recorded activities in 2006. The hacker group published its messages by falsifying 2307 state- and non-state websites in 2006. One of the members of the group was caught while searching by the police on suspicion of a stolen computer in Diyarbakir, in 2008. The police found encrypted confidential documents, passports, malware code-named “Poison Ivy” and video recordings, which belong to the General Staff, National Intelligence Agency, and Gendarmerie in the captured person. During the search done at captured person’s home, 924 CD-ROMs, 57 DVDs, 22 hard disks, and two computers containing confidential information were seized. In the inquest, Hacker declared that he obtained this information by placing the “Poison Ivy” malware on porn websites, by taking advantage of some vulnerabilities he could infiltrate the computers of the intelligence service and military members. With the information given by the captured person, the courier who carried this information to the PKK headquarters was also caught.

The PKK’s other hacker group is the organization operating under the name “Mesopotamia Hackers”. Ankara Police Department Intelligence and Anti-Terrorism Branch offices and General Directorate of Security, Department of Cybercrime determined that due to so-called congress decisions of the terrorist organization, hackers who were active in PKK/KCK were united under the umbrella of the “Mesopotamia Hackers”. During the operation organized by the Ankara Chief Public Prosecutor’s Office on October 1, 2020, 21 people were detained because of conducting propaganda on behalf of the PKK/KCK terrorist organization via cyber attacks.

In the statement made by the police, it was pointed out that suspects realized unauthorized access to the websites of 411 public institutions and organizations and 14,271 legal entities in 81 provinces and made a financial claim on behalf of the organization for whom they conducted propaganda.

On November 6, 2020, simultaneous operations were conducted in 8 provinces against the members of "Mesopotamia Hackers". The captured terrorists confessed their guilt concerning hacking the websites of many public institutions and private sector.

In one of the studies related to the possible threat size of the PKK, it was argued that the hacker groups belonging to or are under the control of the organization have the potential to pose a threat to Turkey's nuclear power plants, which will be put into service in the future. Moreover, they have also been found to be quite dangerous, as they have the ability to use both kinetic and cyberattacks to paralyze critical infrastructure.

Another terrorist organization that is fighting against Turkey is the ISIS organization, which also has a great ability to use the virtual world quite intensively. ISIS organization made extensive use of the media and notably, the Internet media. Especially, to reach the Turkish community, ISIS published an electronic journal that is called "Konstantiniyye". The organization used this journal as a propaganda tool, to attract people who speak Turkish and live outside of Turkey, and are exposed to the pressures of Islamophobia. Six issues were published from the inception of the journal in 2015 until December 2020. ISIS organization prefers to use the Internet, social media, and mobile apps to recruit militants from the Turkish community (it has gathered around 2100 militants from Turkey), to fund and communicate with its members who are in Turkey. The first serious cyber-attack of ISIS in Turkey took place on the websites of the Association of Public Hospitals and also posted messages praising the organization on the hijacked websites. The organization announced

that if the Turkish army continues operations against it, it will launch a cyberattack on government websites and banks. ISIS's "Cyber Khalifat" group attempted many hacking events in Turkey and tried seizing the bank accounts of VIP customers of large banks, which are active in Turkey, to fund the organization.

The above-given examples reflect only some of the terrorist cyberattacks against Turkey. Turkey, in parallel with the international community, is trying to take measures to combat both cyber terrorism and in general, virtual attacks. The first work done on this issue was the production of legal legislation and the establishment of cooperation agreements with foreign countries concerning cyber security. The country, in parallel with the threat dimension, has focused on both improving the legislation and establishing cybercrime units within the security units since 2010.

The studies regarding the potential of the terrorist organizations that are active and against Turkey indicate that cyber terrorists have the capacity to interfere with critical entities like nuclear facilities. This situation is significant since it shows the level that cyber terrorism has reached. Turkey is one of the progressive countries that are trying to take measures by establishing units in order to combat cybercrime. It is clear that regarding these issues significant progress has been made. Due to its geopolitical position, Turkey is a target of international terrorism. Terrorist organizations that have serious means are looking for defense vulnerabilities to attack Turkey. Besides, considering the development of the cybercriminals, which they reach day by day, it can be claimed that defensive measures would be insufficient and a proactive combat plan is necessary for combatting cybercrime. It has become mandatory to have counter-units that will be one step ahead of cybercriminals in order to avoid major events of destruction.