SUNUŞ

Siber terörizmin tehdit potansiyeli her geçen gün biraz daha artmaktadır. Birçok güvenlik uzmanı ve politikacı, siber terörizmin gelişmiş ve gelişmekte olan ülkelerde devletin sivil, askeri, finansal ve hizmet sektörlerindeki teknolojik altyapılarına ve özel bilgisayar sistemlerine saldırı ihtimalinin olduğunu açıklamıştır.

Bu potansiyel tehdit had safhadadır fakat ortaya atılan bütün karanlık kehanetlere rağmen kayıtlara geçmiş gerçek anlamda bir siber terörizm örneği bulunmamaktadır. Bu durum şu soruyu akla getirmektedir: "Bu tehdit ne kadar gerçek?"

Modern dönemlerin en büyük iki korkusu "siber terörizm" adı altında birleşmiştir. Teknolojik araçlardan ve modern alışkanlıklardan mağduriyet korkusu, bilgisayar teknolojilerine olan güvensizlik ve endişe ile birleşerek bir siber terörizm korkusu yaratmıştır.

11 Eylül saldırılarından önce yaşanan birkaç olay Amerikan ordusunda ve enerji sektöründeki bilgisayar teknolojilerinin zaaflarını ortaya çıkarmıştır. Bu zaaflar askeri sistemlere bir güvensizlik yaratmıştır. 11 Eylül saldırılarından sonra siyasi, ticari ve güvenlik çevrelerinden gelen uyarılar, terör ve güvenlik söylemleri siber terörizmin yakın gelecekteki belirgin tehlikesini ön plana çıkarmaktadır.

Siber terörizm, hiç kuşkusuz sinsiliği, kitlesel anlanda hasar verebilme potansiyeli, psikolojik etkisi ve medyatik cazibesiyle modern teröristler tarafından ilgi görmektedir. Ancak yine de siber korku çok fazla abartılmaktadır. Teröristler tarafından ulusal altyapıların kritik birimlerine, siber terörizm adını hak edecek derecede, bilinçli ve organize biçimde gerçekleştirilen bir siber saldırı mevcut değildir.

Nükleer silahlar, hassas askeri sistemler ve dünyanın önde gelen ulusal teşkilatlarının bilgisayar sistemleri oldukça iyi korunmaktadır. Bu sistemlere dışarıdan erişmek çok zordur. Bununla birlikte özel sektördeki sistemler daha az güvenli ve muhtemel tehlikelere karşı daha hassastır.

Siber terörizm potansiyelinin abartıldığı düşünülebilir. Ancak böyle bir tehdidi inkar etmek ya da görmezlikten gelmek yanlıştır. Terörle mücadelede elde edilen başarı teröristleri siber terörizm gibi olağandışı yöntemlere yöneltebilir.

Türkiye gelişmiş ülkeler kadar olmasa da siber terörizm tehdidini gözardı edemez. Çünkü teknolojik sistemlerde güvenlik açığı oldukça fazladır. İç ve dış terörist unsurların hedefleri arasında yer alan Türkiye'nin resmi ve özel kuruluşlarının teknolojik altyapıları

daha güvenli hale getirilmezse, siber terörizm tehdidi her geçen gün daha da artacaktır.

Bu rapor, TASAM Genel Müdürü Atilla SANDIKLI ve Uzman Yardımcısı Gökhan YİVCİGER taafından, United States Institude of Peace (USIP)'in Mayıs 2004 tarihinde yayınladığı "Syberterrorism, How is the Real Threat" adlı çalışmadan faydalanılarak hazırlamıştır. Siber Terörizm Raporu'nun devletimize ve milletimize faydalı olması dileğiyle hürmetlerimi sunarım.

Saygılarımla,
Süleyman ŞENSOY
TASAM Başkanı

RAPORU

GİRİŞ

Siber terörizm tehdidi, dünya çapında medyanın, güvenlik çevrelerinin ve bilgi teknolojisi uzmanlarının ilgisini çekmektedir. Bazı gazeteciler, politikacılar ve uzmanlar siber teröristlerin bilgisayar altyapılarına müdahale ederek barajlardan trafik sistemlerine kadar bir çok altyapıya zarar verebileceklerini ileri sürmektedirler. Bunun sonucu olarak, siber terörizmin milyonların yaşamını engelleyebileceği ve küresel güvenliği tehdit edbileceği yönündeki senaryolar oldukça popüler hale gelmektedir. Fakat bütün bu karanlık kehanetlere rağmen bugüne kadar resmi kayıtlara geçmiş tek bir siber terörizm örneği bulunmamaktadır.

Siber terörizmin ortaya çıkardığı bu tehdit ne kadar gerçek? Gelişmiş toplumlar, hayati öneme sahip altyapıları bilgisayar ağlarına çok fazla bağımlı olduğu için kaçınılmaz olarak siber terörizmden korkmaktadır. Teknoloji ihtiyacını çoğunlukla gelişmiş endüstrilerden karşılayan Türkiye'nin de gün geçtikçe bilgisayar altyapılarına bağımlılığı artmaktadır. Bugüne kadar Türkiye'deki bilgisayar sistemlerine zarar vermiş saldırılar, hekırların dünya çapına yaydığı bilgisayar virüslerinden ibaret olsa da, siber terörizm potansiyeli gelecekte endişe verici boyutlara ulaşabilir.

Hekırlar terörist amaçlarla motive olmasalar da, tek başlarına özel bilgisayarlara, kamu ve özel sektör bilgi sistemlerine ulaşarak zarar verebilmektedirler. Teröristler de teorik olarak, hekırların yöntemlerini takip ederek resmi birimlerin ya da bireylerin bilgisayar sistemlerine zarar verebilirler; askeri, finansal ve servis sektörlerini kullanılamaz hale getirebilirler.

Bilgi teknolojilerine giderek artan bağımlılık beraberinde yeni zafiyet alanları ortaya çıkarmıştır. Böyle bir durum teröristlere ulusal güvenlik ve hava kontrol sistemleri gibi hedeflere yönelme fırsatı vermektedir. Özellikle vurgulamak gerekirse, "bir ülke teknolojik olarak ne kadar gelişmiş ise altyapı sistemlerine yapılacak siber saldırılara karşı hassasiyet de o kadar artar".

Siber terörizmin potansiyel tehlikeleri karşısında duyulan endişeler yerindedir. Ancak bu durum, özellikle uluslararası medyanın çok fazla ön plana çıkardığı telaşın mantıklı ve makul olduğu anlamına gelmemelidir. Medyada sıkça yer alan bu korkular gerçekçi değildir ve fazla abartılmaktadır. Buna ek olarak, siber teröristlerin potansiyel zararları ile gerçek zararları arasındaki ayrım göz ardı edilmektedir. Bazı hekırların yapmakta olduğu saldırılar çoğunlukla siber terörist saldırılarla karıştırılmaktadır.

Bu rapor, siber terörizm tehdidinin bugünkü ve gelecekteki durumunu, Türkiye'deki

resmi ve özel kuruluşların teknolojik altyapılarına potansiyel etkilerini değerlendirmekte ve incelemektedir. Rapor, siber terörizmin neden çok fazla insanın dikkatini çektiğini, hangi durumların "siber terörizm" tanımlamasına uygun olduğunu ve gelişmiş ülkelerin siber saldırılara karşı hassasiyetini açıklamaktadır. Türkiye'deki potansiyel tehdidin değerlendirmesini yaparak, kanıtlarını sunmaktadır. Konuyla ilgili daha önce yapılmış çeşitli çalışmaların ve yayınların yaratmış olduğu korkuların ve endişelerin yerinde olup olmadığı incelenmektedir. Sonuç bölümünde ise, gelecekte Türkiye'nin siber terörizmin hedefi olma durumu ve gerçek tehlikelere karşı nasıl tedbir alması gerektiği anlatılmakta ve abartılmış korkuların etkisinde kalmamak için uyarılarda bulunulmaktadır.

SİBER TERÖRİZMİN TEHDİT POTANSİYELİ

Siber terörizm söylemi, 1990'ların başında, internet teknolojilerinin hızla büyümeye başladığı, "bilgi toplumu" tartışmalarının yapıldığı, teknoloji ve bilgisayar ağına fazlaca bağımlı olan ABD'nin karşılaşabileceği riskleri inceleyen çalışmaların arttığı dönemde başlamıştır. ABD Ulusal Bilim Akademisi'nin 1990'ların başında yayınladığı rapor bilgisayar güvenliği üzerine şu yorumu yapmaktadır: "Risk altındayız. ABD'nin bilgisayarlara bağımlılığı giderek artmaktadır... Yarının teröristi bir klavye ile bir bombanın yaratacağı zarardan daha fazlasını yaratabilir." Ayrıca, bu yorumda "elektronik Pearl Harbor" prototip terimi kullanılmış ve Amerika'nın tarihsel travması ile bilgisayar saldırıları arasında paralellik kurulmuştur. Bir teknoloji devi olan ABD'nin bu endişeleri zaman içinde diğer gelişmiş ülkelere de sıçramıştır. Teknoloji bağımlılığı artan ve bilgisayar güvenlik önlemlerine yeterince önem vermeyen Türkiye'nin de yakın gelecekte bu endişelere kapılması muhtemeldir.

11 Eylül saldırılarından sonra terörizm ve güvenlik söylemleri, siber terörizm tehdidi endişelerini arttırmıştır. Bu anlaşılabilir bir durumdu. Dünya çapında daha da korkunç saldırılar beklenmekteydi. Terörist örgütler büyük çaplı zararlar vermek için siber terörizmi kullanabilirlerdi.

Uzman politik, ekonomik ve psikolojik birimler bir araya gelerek siber terörizm tehdidini araştırmaktadır. Psikolojik perspektife göre modern dönemlerin en büyük iki korkusu "siber terörizm" adı altında birleşmiştir. Modern araçlardan ve alışkanlıklardan kaynaklanan mağduriyet korkusu, bilgisayar teknolojilerine olan güvensizlik ve endişe ile birleşerek siber terörizm korkusunu yaratmıştır. Bilinmeyen bir tehdidin bilinenden daha korkutucu olduğu açıktır. Buna rağmen siber terörizm doğrudan bir şiddet tehdidi sunmamaktadır; fakat tedirgin toplumlara yapacağı psikolojik darbe, terörist bir bombanın etkisi kadar

zarar verici olabilir. Daha da ötesi siber saldırılara karşı mücadele çalışmaları, en büyük ve gerçek tehdidin bilinmezlikten, bilgi eksikliğinden ve daha da kötüsü yanlış bilgilerden kaynaklandığını ortaya çıkarmıştır.

Siber terörizme odaklanmanın bir de politik boyutu vardı. Siber terörizm ile ilgili güvenlik tartışmaları her zaman için siyasi aktörlerin ilgisini çekmiş ve indirgemeci bir yaklaşımla değerlendirilmiştir. Bu açıdan bakıldığında siber terörizm zaman zaman küresel siyasetin ve "güç" unsurunun önemli bir parçası haline getirilmiştir.

Örneğin, ABD'de Pentagon'a yakınlığıyla bilinen Potomac Enstitüsü'nde terörizm araştırmacısı olarak çalışan Yonah Alexander, Aralık 2001'de bir "Irak Ağı"nın varlığını duyurmuştu. Yüzün üzerinde web sitesini içeren bu ağ Irak tarafından 1990'ların başında dünyanın bir çok bölgesinde etkin hale getirilmişti. Bu ağ bir çok servisin bilgisayar sistemlerine saldırarak onları erişilemez, kullanılamaz ya da onarılamaz hale getirmekteydi. DoS (Denial of Service) saldırıları da denilen bu girişim Amerikan şirketlerini hedef almaktaydı. Yonah Alexander'ın iddiasına göre Saddam Hüseyin elindeki bu siber silahı kullanmaktan çekinmezdi; ancak ne zaman kullanacağı belirsizdi. Böyle bir silah karşısında da ABD ilk hedeflerden birisi olacaktı.

Daha sonradan bu yazarın maksadının, "siber terörizme vurgu yaparak, Irak'a karşı saldırgan bir tutum izleyen Amerikan politikalarını desteklemek olduğu" görüldü. Bugüne kadar "Irak Ağı"nın varlığına ilişkin tek bir kanıt bulunamamıştır. Siber terörizm, bu örnekte uluslararası siyasete meşruluk zemini yaratma çabalarının bir parçası olarak kullanılmıştır.

Siber terörizmle mücadele fazlaca politize edilebilir bir konu olmanın yanında ekonomik getirisi de oldukça fazladır. Başta ABD olmak üzere birçok gelişmiş devletin teknoloji endüstrileri siber terörizmle mücadele etmek için alarma geçmiştir. Düşünce kuruluşları kapsamlı projeler tasarlamakta, raporlar hazırlamaktadır. Özel şirketler telaş içinde güvenlik danışmanlık birimleri oluşturmakta, özel ve kamusal hedefleri korumak adına yeni güvenlik yazılımları geliştirilmektedir. 11 Eylül saldırılarının ardından Amerika Federal Hükümeti altyapı güvenliği için 4,5 milyar dolar talep etmiştir ve FBI binden fazla "siber müfettişiyle" kontrol sağlamaya çalışmaktadır.

Bu hususta Türkiye'de fazla bir hareketlilik yaşanmamaktadır. Sadece telekomünikasyon endüstrisi ve bazı özel şirketler kendi güvenlikleri için önlemler almaktadır. Bu nedenle, kamusal hizmet sektöründe elektrik güç üniteleri başta olmak üzere, bazı kritik altyapılar tehlikelere hassas durumdadır.

11 Eylül saldırılarından önce George W. Bush yakın gelecekte siber teröristlerin ABD'ye muhtemel saldırıları konusuna dikkat çekmeye çalışmıştır. Başkan adayı olarak yapmış olduğu uyarıda Amerikan ordusunun birçok tehdit tarafından kuşatılmış olduğunu vurgulamıştır. Kitle imha silahlarının yayılması, füze teknolojilerinin gelişmesi ve siber terörizmin yükselişi bu tehditler arasındadır. Bu şekilde yapılan açıklamaların, politik açıdan meşruluk zemini yaratma çabası olduğu vurgulanabilir.

11 Eylül sonrasında George W. Bush Beyaz Saray'da Siber Güvenlik Dairesi'ni oluşturmuş ve başına da terörle mücadele eski koordinatörü Richard Clarke'ı atamıştır. İç Güvenlik Departmanı Direktörü Tom Ridge'in Nisan 2003'te yapmış olduğu uyarı, "Teröristler ağ bağlantılı bilgisayarların başında oturarak dünya çapında bir hasara yol açabilirler, büyük bir ekonomik sektörün güç şalterini kapamaları için bomba ya da patlayıcılara ihtiyaçları yok" şeklindeydi. Bu mesaj ABD içinde büyük etki yarattı. Örneğin, 11 Eylül saldırılarının ikinci yıl dönümde, "Ulusal Şehirler Birliği" (National League of Cities) adlı kurum tarafından 725 şehir üzerinde yapılan incelemede, yerel yetkilileri biyolojik ve kimyasal saldırılardan sonra en çok endişelendiren tehdidin siber terörizm olduğu anlaşılmıştır.

Amerikan medyası bu konuyu ağız birliği eder biçimde, felaket senaryoları üreterek manşetlerine taşımıştır. Washington Post'un Haziran 2003'teki manşetinde olduğu gibi: "El Kaide tarafından gerçekleştirilen siber saldırılar korku yarattı. Uzmanlar uyarıyor! Teröristler internet yoluyla kan dökmenin eşiğindeler". Medyanın bu korkuyu popüler hale getirmesiyle, roman ve senaryo yazarları da bu dramatik potansiyelin farkına varmıştır. 1995 yapımı bir James Bond serisi olan Golden Eye ve 2002 yapımı Code Hunter adlı Hollywood filmleri ile Tom Clancy ve Steve R. Pieczenik'e ait Netforce adlı roman siber terörizm senaryolarını geniş kitlelere ulaştırmışlardır.

Medya, hekırların resmi web sayfalarına yapmış olduğu saldırıları, yarattığı bilgisayar virüslerini, özel şirketlerin gizli bilgilerine ulaşmalarını sıklıkla siber terörizm örneği olarak duyurmuştur. Türk medyası ise siber terörizm malzemesiyle yerel bazda bir sansasyon yaratma girişiminde henüz bulunmamıştır, çünkü toplumda henüz fazlaca bir tehlike endişesi bulunmamaktadır.

SİBER TERÖRİZMİN TANIMI

Özellikle Amerikan kaynaklı küresel medyayı incelediğimizde siber terörizm teriminin çoğunlukla yanlış yerde kullanıldığını görmekteyiz. Siber terörizmin tehlike potansiyelini anlayabilmemiz için öncelikle bu terimi doğru bir şekilde tanımlamamız gerekmektedir.

"Siber Terörizm"in net ve tutarlı biçimde anlaşılmasına engel olan yanlış fikirlerin altını öncelikle çizmekte fayda vardır. İlk olarak yukarıda da bahsedildiği üzere siber terörizm tartışmaları kitlesel medya tarafından yönlendirilmektedir. Yazarlar yeni kavramları tutarlı ve mantıklı biçimde tanımlamak yerine sansasyon peşinde koşmaktadırlar.

İkinci olarak, bilgisayar sistemleri üzerine yapılan tartışmaların yepyeni kavramlar, terimler doğurması çok moda olmuştur. Bir başka sözcüğün önüne "siber", "computer" veya "bilgi" sözcüklerini getirerek yeni bir kelime yaratılmaktadır. Siber suç, bilgi savaşı, ağ savaşı, siber terörizm, siber bunalım, dijital terörizm, siber taktik, bilgisayar savaşları ve siber saldırı gibi kavramlar bazı askeri ve siyasi stratejistlerin de tanımladığı gibi küresel medya tarafından çağımızın "yeni terörizm"i olarak tanımlanmaktadır.

Bir çok bilim adamı tarafından siber terörizm hakkında yapılan açıklamalar konuya açıklık kazandırmıştır. En dikkate değer açıklama, Amerikalı bilgisayar bilimi profesörü Dorothy Denning'in makalelerinde yer almıştır.

Siber terörizm, siber boşluk ve terörizmin bileşimidir. 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. Daha da ötesi, bir saldırının siber terörizm olarak tanımlanması için bireye ya da mala karşı şiddet içermesi gerekmektedir. En azından "korku yaratacak kadar hasara" yol açmalıdır. Siber terör ölümcül olan ya da fiziki hasara yol açan, şiddetli ekonomik kayba neden olan saldırılar olarak örneklenebilir. Kritik altyapı odaklarına yapılan ciddi saldırılar yarattığı etkiye göre siber terörizm olarak tanımlanabilir. Önemli olmayan servislere verilen rahatsızlıklar siber terörizm olarak tanımlanamaz.

"Siber terörizm" ile "hekırlık" arasındaki farkın anlaşılması son derece önemlidir. Kişisel ya da kurumsal bilgisayar sistemlerine zarar veren, kayıtlı bilgileri yok eden hekır saldırıları, siber terörizmde olduğu gibi politik maksatlarla motive olmamaktadır. Protesto amacı taşımazlar, öldürmek ya da yaralamak gibi amaçları yoktur. Ancak, hekırlık siber terörizmin tehlike potansiyeli hakkında ipucu vermektedir. Teröristlerin, hekırların kullandığı metotlara benzer metotlar kullanarak büyük hasara yol açabileceklerini göstermektedir.

TERÖRİST ÖRGÜTLER İÇİN SİBER TERÖRİZMİN ÇEKİCİLİĞİ

Terörist örgütler için siber terörizm birkaç nedenden dolayı çekici olabilir.

Öncelikle geleneksel anlamdaki terörist metotlardan daha az maliyetlidir. Terörist

örgütün ihtiyacı olan tek şey ağ bağlantılı bir kişisel bilgisayardır. Silah ya da patlayıcı temin etmek zorunda değildirler. Bunun yerine yarattıkları bilgisayar virüslerini telefon hatları veya kablo bağlantıları aracılığıyla yayabilirler.

İkinci olarak teröristler örgütler, siber terörizm aracılığıyla saldırgan kimliklerini bilinen anlamdaki terörizm metotlarına kıyasla daha iyi gizleyebilmektedirler. Diğer bütün internet gezginleri gibi teröristler de kendisine bir takma ad vererek güvenlik birimlerinin ve polis teşkilatlarının kimliklerine ulaşmasını engelleyebilmektedirler. Böylesine bir siber boşlukta saldırganı sınırlayacak fiziki bariyerler, kontrol noktaları, sınır kapıları ya da gümrükler bulunmamaktadır.

Üçüncü olarak hedef seçilebilecek noktaların sayısı oldukça fazladır. Siber teröristler, hükümetler, silahlı kuvvetler ile diğer güvenlik ve istihbarat örgütleri, kamu hizmeti yapan kuruluşlar, özel hava yolları, bireyler ve bilgisayar ağları gibi hedeflere yönelebilirler. Teröristlerin bu kadar çok potansiyel hedef arasında zayıf ve savunmasız bir nokta bulma olasılığı fazladır. Yapılan bazı çalışmalara göre elektrik şebekelerinin kritik altyapı sistemleri çok karmaşıktır, savunulmaları ve bütün zaaflarının giderilmesi olanaksızdır. Bu nedenle de siber saldırılara çok açıktırlar.

Siber terörizmin bir başka çekiciliği de uzaktan kumanda edilebilir olmasıdır. Siber terörizm fiziksel bir eğitim gerektirmez, ölüm riski yoktur, psikolojik açıdan zorlayıcı değildir. Bu özellikleri sebebiyle terörist örgütler için yeni üyeler kazanmak kolaydır.

Son olarak, I LOVE YOU virüsü ortaya çıkıp, küresel bazda yayıldığında anlaşıldı ki; Siber terörizm bilinen anlamda terörist metotlarından çok daha fazla insana zarar verebilmekte ve bir teröristin istediği gibi medyayı fazlasıyla etki altına alabilmektedir.

SİBER TERÖRİZME KARŞI ARTAN HASSASİYET

ABD'nin Ulusal Güvenlik Ajansı (NSA), 1997 yılında "Eligible Receiver" kod adlı bir tatbikat yaptı. Tatbikat kapsamında bilgisayar hekırlarından meydana gelen otuz beş adet "kırmızı takım" oluşturdu. Tatbikatın sonucu dehşet vericiydi. Hekırlardan belirli kurallar çerçevesinde Amerikan ulusal güvenlik sistemlerini karıştırmaları istendi ve ilk hedef olarak da Hawaii'deki Pasifik Komutanlığı gösterildi. Takım üyelerinin sadece bilgisayar yazılımlarını ve internetten kolayca elde edilebilen hekır araçlarını kullanmalarına izin verildi. Tatbikatın sonucu gösterdi ki; "Kırmızı Takım" internet üzerinde herkese açık olan hekır araçlarını kullanarak Pasifik bölgesindeki bütün Amerikan askeri kontrol ve komuta sistemlerine zarar verebilirdi. Askeri açıdan tek başına böyle bir olasılık bile korku vericiydi. Ancak,

tatbikatın sonuçları, daha fazla hassasiyetin olduğunu gösterdi. Aynı yöntem ve teknikler kullanılarak telekomünikasyon sistemleri, elektrik güç üniteleri gibi özel sektör altyapı sistemlerinin çökertilebileceği de ortaya çıktı.

Dan Verton tarafından 2003 yılında kaleme alınan, "Black Ice: The Invisible Threat of Cyber-Terror" adlı kitapta enerji sektörlerindeki bu büyük hassasiyet detaylı bir biçimde işlendi. Verton'un görüşüne göre; ABD'ye karşı yapılacak siber terör saldırılarında Amerikan enerji sektörünün, ilk düşen domino taşı olma ihtimali yüksektir. Kitap bu tarz bir saldırının boyutları ve etkilerinin bilinen anlamdaki fiziksel terörist saldırıların etkilerinden çok daha fazla olabileceğini vurgulamaktadır. Verton'un iddiasına göre orta büyüklükte bir şirket bir yılda bir milyon civarında siber tacize maruz kalmaktadır. Bu sayı sadece ciddiye alınan ve sistemlere zarar veren tacizlerin sayısıdır. Amerikalı bir araştırma kuruluşunun yaptığı incelemeye göre; 11 Eylül saldırılarını takip eden altı ay içinde enerji endüstrisinde yer alan şirketlerin siber tacizlere diğer endüstrilere oranla iki kat fazla maruz kaldığı ortaya çıkmıştır. Bütün siber tacizlerin içinde acil müdahale gerektirenlerin oranı ortalama olarak yüzde 12.5'tir.

İnternet altyapılarının güvenlik sistemlerindeki açıklar sürekli olarak tespit edilmektedir. Siber güvenlik konusunda dünya lideri olan Symantec firmasının görüşüne göre; ABD genelinde internet altyapılarındaki açıklar, 2002 yılında bir önceki yıla kıyasla yüzde seksen oranında artış göstermiştir. Ancak yine de tam anlamıyla siber terörizm tanımlamasına uygun bir saldırı kayıtlara geçmemiştir. Bunun nedeni, teröristlerin böyle bir boşluktan ve zayıflıktan yararlanabilecek kadar "beceriye erişememiş olması" ile bu amaçlara yardımcı olabilecek kapasitedeki hekırların ve virüs yazıcılarının terörist eylemlere sempatik bakmamasıdır. Bu iki grup ortak noktada buluşurlarsa sonuç çok yıkıcı olabilir.

Bir başka endişe ise, yazılım sistemleri üreten firmaların veya kişilerin bunu terörist amaçla tasarlayıp resmi yönetim birimlerine kurmaları ihtimalidir. Böyle bir endişe, Mart 2000'de önemli bir olayla gerçeğe dönüşmüştür. Japonya Metropol Polis Departmanı için 150 polis aracını merkezden takibe alabilen bir yazılım, 1995 yılında Tokyo metrosuna gaz bombası atan ve on iki kişinin ölümüyle, altı binden fazla kişinin yaralanmasıyla sonuçlanan saldırıyı gerçekleştiren Aum Shinryko adlı bir grup tarafından tasarlanmıştır. Bu durum ortaya çıktığında, grubun 115 polis aracının takibiyle ilgili bilgileri elinde bulundurduğu tespit edildi. Daha da ötesi, en az seksen adet Japon firmasına ve on kadar hükümet birimine yazılım sistemi tasarlamışlardı. Grup başka yazılım firmalarının kritik kademelerinde örgütlenerek izlerini gizleyebilmiş ve bu yöntemle bir çok özel ya da resmi birim için "Truva

atları" hazırlayabilmişdi.

Bu konuda alınması gereken önlemler hakkında bir değerlendirme yapıldığında, dışarıdan yazılım ve donanım desteği alan Türk Silahlı Kuvvetleri'nin güvenlik önlemleri örnek olarak gösterilebilir. Üniversitelerden, çeşitli ihtisas kurumlarından alınan destek çalışmaları TSK'nın bilgi işlem uzmanları denetiminde gerçekleştirilmektedir. Dolayısıyla herhangi bir casus sistemin yerleştirilmesi engellenmektedir. TSK şimdilerde uzman mühendislerinden oluşan birimleriyle çoğu yazılımlarını kendisi geliştirmektedir ve şu an için güvenlik endişesi taşımamaktadır. Ancak teknik altyapı güvenliği, donanım özelliklerinden başlayarak değerlendirilmesi gereken bir konudur. Son kullanıcıya yönelik yazılımlar kadar kullanılan işletim sistemi ve bu sistemin üzerinde çalıştığı fiziksel altyapı özellikleri de ciddi tehdit unsurları içeren hassasiyetlere sahip olabilir. Bu tür hassasiyetler son kullanıcıya yönelik yazılımlardan daha büyük riskler içerir.

11 Eylül saldırılarından sonra, ABD kökenli Ticari Yazılım Birliği'nin (Business Software Alliance) 395 bilgi teknolojisi profesyoneliyle yaptığı görüşmeler sonucunda Amerikan hükümetinin siber saldırılara karşı güvenlik sağlamakta yetersiz kaldığı anlaşılmıştır. Uzmanların yüzde 49'u bu tarz bir saldırının çok yakın olduğu görüşündedir. Yüzde 55'i ise 11 Eylül saldırılarından sonra siber saldırı tehdidinin oldukça arttığını söylemiştir. Yüzde 59'una göre; firmalarının bilgisayar ve internet güvenliğini bireysel olarak sağlayanlar, özellikle 11 Eylül saldırıları sonrasında çok büyük risk altındadırlar. Yüzde 72'sine göre ise devletin aldığı güvenlik önlemleriyle siber saldırı riski arasında büyük boşluk bulunmaktadır. Yüzde 84'ü hükümetin bilgisayar güvenlik sistemleri için daha fazla kaynak ayırması gerektiği görüşündedir. Öncelikli hedefler arasında Wall Street gibi ulusal finans kurumlarının, büyük ulusal bankaların olduğunu düşünenlerin oranı yüzde 74 civarındadır. Komünikasyon ağı, trafik kontrol sistemleri, baraj kontrol sistemleri ve elektrik güç üniteleri gibi hedeflere öncelikle yönelinebileceğini iddia edenlerin oranı ise yüzde 66 civarındadır.

31 Ocak 2004 tarihli Washington Post gazetesinde yer alan bir araştırma uzmanların yukarıdaki kuşkularını doğrular niteliktedir. Amerikan Hükümetine bağlı teknolojik reformlar alt komitesi yönetimindeki araştırma, federal birimlerdeki bilgisayar güvenlik sistemlerini inceleyerek not vermiştir. Not verme sistemi basitçe, kurumların çalışanlarını güvenlik konusunda ne kadar eğittiğine ve özel bilgilere ulaşımın sınırlandırılması esasına dayandırılmıştır. Araştırma sonunda çoğu federal birim çok düşük notlar almıştır. Yirmi dört federal birim içinde en düşük notu alan İç Güvenlik Departmanı (Departmant of Homeland Security) olmuştur. Yine düşük not alan bir başka birim ise Adalet Departmanı

(Justice Departmant) olmuştur.

Yapılan bu tarz çalışmalar medyanın da ilgisini çekmiş ve halkta siber terörizm korkusunu ateşlemiştir. ABD'de bin kişiye yönelik olarak yapılan bir araştırmada neredeyse yarısının siber terörizm endişesi yaşadığı tespit edilmiştir. Araştırma 2003 Ağustos ayının başında, yeni virüslerin dünya geneline yayılıp birçok bilgisayara zarar vermesinden önce gerçekleştirilmiştir. Bununla birlikte, virüs saldırıları "Siber Terör" tanımının tam olarak içinde yer almamaktadır. Gayet tabi ki virüsler herhangi bir siber terör saldırısında araç olarak kullanılabilirler. Ancak kesin hedefli, sistematik bir terörist saldırı aracı olarak virüs yazılımı, özel amaçla hazırlanmış bir silah olarak düşünülmelidir. Bu açıdan bilişim toplumunun genelinde etkili olan, her gün bir yenisini duyduğumuz virüsler bu kapsamın dışında düşünülmelidir. Bu tip virüsler daha çok propaganda aracı olarak bilgi kirliliği yaratmak veya genel bilgi iletişimini aksatmak için kullanılabilirler.

SİBER TERÖR TEHDİDİNİN BÜYÜKLÜĞÜ

Siber terörizm konusunda endişe yaratan bütün bu çalışmalar ve istatistikler içinde en önemli olanı, bugüne kadar her hangi bir siber terörizm vakasının kayıtlara geçmemiş olmasıdır. Kamu kuruluşlarına, ulaşım sistemlerine, nükleer enerji ünitelerine, elektrik güç ünitelerine veya kritik ulusal altyapı bileşenlerine herhangi bir siber terörizm hareketi gerçekleşmemiştir. Siber saldırılar oldukça yaygındır; fakat teröristler tarafından gerçekleştirilmemiştir ve siber terörizm olarak tanımlanacak kadar zarar vermemiştir.

Türkiye açısından bugüne kadar meydana gelmiş en büyük tehdit kısa sürede dünya çapına yayılan virüs saldırılarından ibarettir. Bu saldırılar kişisel ya da kurumsal bilgisayarların yazılım veya işletim sistemlerine zarar vererek kimi zaman bunları kullanılamaz hale getirmektedir.

Bir başka tehlike ise artık çok yaygınlaşmış olan ve doğrudan internet sitelerini hedef alan hekır saldırılarıdır. Ancak bütün bu saldırılar sistemlerde geçici aksaklıklara yol açabilecek kapasitededir. Bütün olarak bir kurumsal teknolojik alt yapıyı çökertecek düzeyde değildir. Siber terörizmin mevcut tehlike potansiyeli Türkiye açısından büyük bir endişe yaratmamalıdır, ancak güvenlik sistemlerinin her yeni gelişmeye karşı güncellenmesi ihmal edilmemelidir.

Afganistan'daki operasyonlarda ele geçirilen El Kaide'ye ait bilgisayarlar Amerikan birliklerini oldukça şaşırtmıştır. Örgütün beklediklerinden çok daha fazla teknolojik donanıma sahip olduğu görülmüştür. Bilgisayarlarda mühendislik yazılımları, Avrupa ve Amerika'daki

bazı stadyumların teknik yapıları, nükleer güç üniteleri hakkında bilgiler ve elektronik baraj sistemlerinin özellikleri gibi veriler bulunmuştur. Ancak örgütün bilgisayarları siber terör saldırıları için değil, diğer fiziki saldırıların koordinasyonu ve aralarında haberleşmeyi sağlamak maksadıyla kullandıkları tespit edilmiştir.

Ne El Kaide ne de bir başka terörist örgüt, bugüne kadar ciddi bir siber saldırı girişiminde bulunmamıştır. Uzmanlara göre; bugüne kadar en ciddi zarar, panik ve endişe yaratan saldırılar bireysel hekırlardan gelmiştir. Bu hekırlar çoğunlukla heyecan arayan ve nam salmak isteyen genç erkeklerdir.

IBM Küresel Güvenlik Analiz Laboratuarı'nın (IBM Global Security Analysis Lab) 2002 yılında yapmış olduğu araştırmaya göre hekırların yüzde 90'ı teknik açıdan sınırlı amatörlerdir, yüzde 9'u yetkisiz girişleri gerçekleştirebilecek kapasitededir. Bunlar dosyalara ve verilere zarar vermemektedirler. Yüzde 1'i çok fazla teknik beceriye sahiptir ve her türlü alana giriş yaparak zarar verebilir. Hekırların çoğu, yazılımların güvenlik sistemlerine ve Microsoft tarafından tasarlanmış işletim sistemlerine zarar vermektedir. Bu tarz tacizler kuruluşları çoğunlukla zor durumda bırakmıştır, ancak kamuyu uyarmak ve yazılım güvenliği uzmanlarını harekete geçirmek konusunda sorumluluk sahibi yapmıştır. Bazı hekırlar, internet üzerindeki elektronik ticarete zarar verebilecek ve web sitelerini bağlantıdan düşürebilecek beceriye sahip olsalar da çoğunluğu yeteri kadar bilgi ve beceriye sahip değildir. Yetenekli olanların ise büyük kargaşa ve yıkım yaratma konusunda hırsları yoktur.

Amerikalı Profesör Douglas Thomas, yedi yıl boyunca bilgisayar hekırları üzerine araştırmalar yapmıştır. Kim olduklarını ve nelerden motive olduklarını anlamaya çalışmıştır. Yüzlerce hekırla görüşerek bir sonuca ulaşmıştır. Bu sonuca göre; hekırların yüzde 99'u siber terörizm açısından her hangi bir risk taşımamaktadır. Çünkü bu tarz bir saldırıyı organize edecek ve uygulamaya koyacak beceriye sahip değildir.

Thomas'ın çalışmaları; Amerika'daki Stratejik ve Uluslararası Çalışmalar Merkezi'nin "Siber Terörizm Riskleri, Siber Savaş ve Diğer Siber Tehdit Değerlendirmeleri" (Assesing the Risks of Cyberterrorism, Cyber War, and Other Cyber Threats) adlı 2002 yılı raporunda da geniş bir şekilde yer almıştır. Raporu kaleme alan Jim Lewis'in görüşüne göre; "Hekırların bütün bir ulusu dizleri üstüne çöktüreceği konusundaki senaryolar çok uzak bir ihtimallidir ve ciddiye alınmamalıdır". Lewis ifadesine şöyle devam etmiştir: "Uluslar, siber terörizm araştırmacılarının onlara tanıdığı krediden çok daha sağlam durumdadır. Altyapı sistemleri, analizcilerin söylediğinin aksine daha esnektir ve kendini onarma becerisine sahiptir; çünkü herhangi bir sorunda rutin görevini devam ettirebilirler."

Çoğu bilgisayar güvenlik uzmanının da vurguladığı gibi, internet kanalıyla ölüme yol açmak neredeyse imkânsızdır. Nükleer silahlar ve diğer hassas askeri sistemlerin ise internetle fiziksel bir bağlantısı yoktur. Bu sebeple dış kullanıcılar bu sistemlere ulaşamazlar. Örneğin Amerikan Savunma Bakanlığı'nın önemli sistemleri internet ortamından, hatta Pentagon'un yerel ağından bile izole edilmiştir. Kullanılacak her hangi bir yeni yazılım öncelikle Amerikan Ulusal Güvenlik Ajansı'nın (National Security Agency) denetiminden geçmektedir.

Türkiye'de Genel Kurmay Başkanlığı ve diğer askeri birimler benzer yöntemlerle altyapılarını internet ortamından izole etmişlerdir. Her birimin kendi içinde ve diğer birimlerle fiber optik kablo ağ bağlantısı bulunmaktadır. "İntranet" adı verilen bu ağ bağlantısı, hem içeriden, hem de dışarından yetkisiz girişlere karşı önlem sağlamaktadır. Her askeri birey kendi görev yetkisi çerçevesinde girişler yapabilmektedir ve istihbarat gibi gizli bilgiler sıkıca korunmaktadır.

11 Eylül'deki uçak kaçırma olayları havayollarının siber terörist saldırılara açık olduğu protestolarına neden olmutur. Siber güvenlik uzmanlarının ifadesine göre bir uçağı uzaktan kumanda yoluyla kaçırmak imkânsızdır. Bu nedenle yüksek teknolojiyi kullanan 11 Eylül senaryolarının gerçekleştirilmesi mümkün görülmemektedir.

Kaygılanılan bir başka husus ise istihbarat birimlerinin güvenliğine ilişkindir; ancak istihbarat birimleri belirli bilgisayarlarını yukarıda belirtildiği gibi internet temasından uzak tutmaktadır.

Bütün bunlar, daha az korunmakta olan elektrik güç üniteleri, petrol boru hatları, ve barajlar gibi nükleer sistemlere kıyasla daha az kabus yaratan hedeflere yönelme ihtimalini ön plana çıkarmaktadır. Bu sistemler çoğunlukla özel sektörün kontrolünde olduğundan devlet sistemlerinden daha az korunaklı gözükmektedir. Dahası, firmalar boru hatlarındaki akışı sağlamak ya da barajlardaki su seviyelerini ayarlamak için internet ağıyla birbirine bağlanan SCADA sistemi adı verilen bir yöntem kullanmaktadır.

Siber terörizmin tehdit potansiyelinin algılanabilmesi için uzmanlar iki sorunun sorulması gerektiğini vurgulamaktadır.

Siber saldırılara karşı korunmasız herhangi bir hedef mevcut mu?

Böyle bir saldırıyı gerçekleştirebilecek beceride ve motivasyonda bir aktör var mı?

Birinci soruya cevap evet şeklindedir. Kritik altyapı sistemleri çok karmaşıktır ve mutlaka

terörist eylemlerin faydalanabileceği bir açık barındırır.

İkinci soruya ise şu şekilde cevap verilebilir. Bahsedilen SCADA sistemini firmanın teknik donanımlı çalışanları dışında kullanabilecek insan sayısı çok azdır. SCADA istismarı ile ilgili bir örnek Nisan 2002'de yaşanmıştır. Avustralyalı bir adam internet bağlantısını kullanarak baraj kapaklarını açmış ve milyonlarca metre küp suyun akışını sağlamıştır. Polis tarafından yakalandığında adamın daha önceden barajlar için yazılım üreten bir şirkette çalıştığı tespit edilmiştir.

Bu olay, terörist grupların istismara meyilli çalışanları kendi saflarına katmalarının mümkün olduğunu göstermiştir. Ancak yine de içeriden yardım alınsa da verilebilecek zarar sınırlıdır. Çünkü elektrik şebekelerinde, petrol/gaz ünitelerinde ve komünikasyon sistemlerinde çalışan işçiler sel, fırtına, hortum gibi doğal afetlere karşı deneyimli olduğu için, insan eliyle verilen bir zararı onarmakta çok zorlanmazlar.

SİBER TERÖRİZMİN BUGÜNÜ VE YARINI

Şu anki siber terörizm tehdidinin çok abartıldığını söylemek yanlış olmaz. Çünkü bugüne kadar tek bir siber terör saldırısı kayıtlara geçmemiştir.

Türkiye açısından tehlike şimdilik uzak gözükmektedir. Kritik resmi birimler güvenlik önlemlerini almıştır. Savunma ve istihbarat birimlerinin bilgisayar sistemleri internet ortamından izole edilmiştir. Özel sektördeki sistemlerde güvenlik eksiği mevcuttur ve saldırılara karşı savunmasızdırlar. Ancak bu sistemler de beklenenden daha çabuk onarılma yeteneğine sahiptirler.

Siber saldırıların pek çoğunluğu bağımsız hekırlar tarafından gerçekleştirilmektedir ve pek azı politik hedef içermektedir. Peki, bu küçük çaplı tehdit neden çok büyükmüş gibi gösterilmektedir?

Birincisi siber terör, siber saldırı gibi kavramlar insanların hayal güçlerine çok çekici gelmektedir.

İkincisi, medyanın hekırlık ile siber terörizm kavramlarını sıklıkla karıştırması ve en küçük olayları abartan başlıklar atmasıdır. Örneğin "16 yaşındaki bir çocuk böyle bir şey yaparsa, kim bilir organize bir terör örgütü neler yapar" gibi gerçeği yansıtmayan başlıklardır.

Bilgisizlik üçüncü faktördür. Siber terörizm, teknoloji ve terörizm eksenlerini birleştirmektedir. Bir çok insan, üst düzey resmi görevli ve kanun koyucular bunu tam

olarak anlamamaktadır ve korkuya kapılmaktadır. Özellikle ABD'de sayısız teknoloji şirketi toplu bir çöküş ve ulusal güvenlik endişesi duyurarak bu çarkı döndürmekte ve federal birimlerden ödenek almaktadır. Hukuki yürütme organları ve güvenlik uzmanları da sıklıkla halkı ulusal güvenlik tehdidine inandırmaktadır.

Dördüncü bir neden ise politikacıların rant amacıyla böyle bir endişeyi gündemde tutmaya çalışmasıdır.

Son bir neden ise bir çok vakaya çok yanlış olarak "siber terörizm" adı yakıştırılmasının kamuoyunda panik yaratmasıdır.

El Kaide'nin modern teknolojik imkanlara karşı ilgisi açıktır. Bin Laden ve diğer yöneticiler siber terörizm hakkında bilgilere sahiptir. 11 Eylül saldırılarından hemen önce Bin Ladin bir Arap gazetesine verdiği demeçte, "yüzlerce Müslüman bilim adamı becerileriyle eylemlere destek vermeye hazırdır" demiştir. Bin Ladin'in mesajlarını Batı dünyasına ileten El Kaide üyesi Şeyh Ömer Bekri Muhammed, bir ifadesinde Bin Ladin'in siber silah konusundaki uyarılarının ciddiye alınmasını tavsiye etmiştir. Teknolojiyi kullanarak kapitalist devletlerin ekonomilerini vurmak, Bin Ladin'in en yakın hedefleri arasındadır.

Siber terörizm gelecekte günümüzdekinden daha fazla bir potansiyele sahip olacaktır ve sanal dünyaların daha da bütünleştiği bir ortamda çekiciliğini arttıracaktır. Örneğin bir terörist grup eş zamanlı olarak bir tren istasyonunda bomba patlatarak, siber yöntemle de iletişim altyapılarına zarar vererek olayın etkisini büyütebilecektir. Tabii bütün bunlar güvenlik tedbirlerinin yetersiz kaldığı durumlarda gerçekleşebilir ve gelecekte böyle bir eylemi gerçekleştirmek, bugün bir web sitesine zarar vermekten daha kolay olabilir.

Mevcut siber terörizm tehdidi karşında fazla endişeye gerek yoktur. Ancak teknolojik gelişmelerin son yıllarda özellikle bilişim sektöründe müthiş atak yaptığı dikkate alınmalıdır. Türkiye'nin bu gelişmelere çok kolay adapte olduğu göz önüne alınırsa, gelecekte siber terörizm Türkiye'de de hedef bulmakta zorluk çekmeyecektir. Özellikle özel sektörde güvenlik zafiyeti olan birimler birincil hedefler arasına girebilecektir. .

Paradoksal anlamda, terörle yapılan mücadelede elde edilen başarı teröristleri siber terörizm gibi olağandışı yöntemlere yöneltebilir. Yapılması gereken, siber terörizm tehlikesini iyi kavrayıp korku ve endişe yaratmadan tehdit potansiyeline uygun çözümler üretmektir.

Sonuç olarak, terör uzmanlarının ifadesine göre; kaçırılan uçaklar, bomba yüklü kamyonlar ve biyolojik silahlar en azından şimdilik siber terörizme kıyasla daha fazla tehlikelidir.

Ancak, 11 Eylül nasıl bütün dünyaya büyük bir sürpriz yaşatmışsa, gelecekte de siber saldırılar bütün dünyaya aynı şekilde büyük bir sürpriz yaşatabilir. Siber terörizm çarpıtılıyor ve abartılıyor olabilir fakat bu onu inkâr etmemiz anlamına gelmemelidir.