Bâkır Emre

Uzman Araştırmacı
Siber Güvenlik Enstitüsü
TÜBİTAK BİLGEM SGE

Türkiye'de Siber Güvenlik

Teknoloji insanoğlunun ilerlemesinde önemli bir itici güç. Teknolojideki gelişmeler ekonomi, sağlık, spor gibi farklı alanların yanı sıra devletlerin mücadeleleri sonucu ortaya çıkan savaşlarda da kullanılıyor. Teknoloji yeni savaş yöntemleri doğuruyor veya var olan savaş algısında değişikliklere yol açıyor. Savaşlar da teknolojik ilerlemenin hız kazanmasına sebep oluyor ve bu iki alan birbirini besliyor. Hatta teknoloji sayesinde savaşlar artık yepyeni bir alanda yapılıyor denebilir.

>>>

Siber uzay, ABD Savunma Bakanlığı'nca "internetin bulunduğu, telekomünikasyon ağlarını ve bilgisayar sistemlerini de kapsayan, birbirine bağlı bilgi teknolojisi altyapılarının olduğu küresel bir alan" olarak tanımlanıyor. Şöyle bir tanımlama da var: "İnsanların bilgisayarlar ve telekomünikasyon sistemleri aracılığıyla herhangi bir coğrafi sınırlamaya maruz kalmadan, birbirine bağlı olma durumu". Siber uzaydan gelebilecek saldırılara ve tehditlere karşı kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan politikalar, güvenlik kavramları, risk yönetimi yaklaşımları ise siber güvenliği oluşturuyor. Düşman olarak belirlenen hedefe siber saldırıda bulunmak, saldırılara karşı savunma yapmak, istihbarat verisi toplamak siber savaş faaliyetlerini oluşturuyor. Siber savaşların ana hedefi ülkelerin güvenlik, sağlık, enerji, ulaşım, haberleşme, su, bankacılık, kamu hizmetleri gibi kritik sektörlerinin bilgi sistemi altyapıları.

Siber Savaşa Karşı Önlemler

Siber ortamda Rusya'nın siber suç araçları, ABD'nin haberleşme istihbaratı konusunda üstünlüğü, Çin'in endüstriyel casusluk kabiliyeti olduğunu biliyoruz. Bu kabiliyetler başka devletler üzerinde siber tehdit oluşturuyor. Dolayısıyla siber tehditler ve siber güvenlik bütün ülkeler için önemli güvenlik unsurlarının başında geliyor. Siber tehditlerin öneminin farkına varan ülkeler gerekli tedbirleri alıyor, stratejilerini, doktrinlerini, altyapı ve organizasyonlarını kuruyor.

Türkiye'deki siber güvenlik yapıları ve faaliyetleri

Bilgi Toplumu Stratejisi 2006-2010

Devlet Planlama Teşkilatı'nın (DPT) koordinatörlüğünde hazırlanan Bilgi Toplumu Stratejisi, Türkiye'nin 5 yıllık süreçte bilgi ve iletişim teknolojilerinden etkin olarak yararlanması ve bilgi toplumuna dönüşmesi için gerekli adımların tespiti için hazırlandı. Siber güvenliğe ait maddeler ek Eylem Planı'nda, 88 no'lu "Ulusal Bilgi Sistemleri Güvenlik Programı" eylemini gerçekleştirme sorumluluğu TÜBİTAK-UEKAE'ye veriliyor. Bu eylem şöyle açıklanıyor:

Siber ortamdaki güvenlik tehditlerini sürekli olarak takip edecek, uyarılar yayınlayacak, bu risklere karşı ne şekilde tedbir alınabileceğine dair bilgilendirme yapacak, risklerin ortaya çıkması durumunda karşı tedbirleri koordine edebilecek bir Bilgisayar Olaylarına Acil Müdahale Merkezi (BOME) kurulacaktır.

Kamu kurumları için gerekli minimum güvenlik seviyeleri kurum ve yapılan işlem bazında tanımlanacak, kurumlar tarafından kullanılan sistemlerin, yazılım ve ağların güvenlik seviyeleri tespit edilecek ve eksikliklerin giderilmesi yönünde öneriler oluşturulacaktır.

Siber Güvenlik Tatbikatları

Kamu ve özel kurum ve kuruluşlar için siber güvenlik farkındalığının artırılması, kurumların siber saldırı anında ve sonrasında koordinasyonlarının sağlanması amacıyla ulusal düzeyde siber tatbikatlar düzenleniyor.

Ülkemizdeki siber güvenlik tatbikatlarının ilki olan BOME 2008 Tatbikatı TÜBİTAK UEKAE bünyesinde faaliyet gösteren TR-BOME koordinatörlüğünde, 20-21 Kasım 2008 tarihlerinde yapıldı. Tatbikata Cumhurbaşkanlığı, Başbakanlık, Adalet Bakanlığı, Sayıştay Başkanlığı, Hazine Müsteşarlığı, Merkez Bankası, Sermaye Piyasası Kurulu, Tapu Kadastro Genel Müdürlüğü'nün ilgili birimleri katıldı.

Daha geniş katılımlı ikinci tatbikat Ulusal Siber Güvenlik Tatbikatı 2011,TÜBİTAK BİLGEM ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) koordinatörlüğünde Ocak 2011'de düzenlendi. Kırk bir kamu ve özel sektör kurum ve kuruluşunun katıldığı tatbikat gerçek saldırılar ve yazılı saldırı senaryoları bölümlerinden oluşuyordu. Gerçek saldırılar kapsamında web güvenlik denetimi, port taraması, dağıtık servis dışı bırakma (DDoS) saldırısı ve siber saldırı kayıt dosyaları analizi olmak üzere dört ayrı faaliyet gerçekleştirildi. Yazılı ortamdaki senaryolarda ise kurum içinden veri sızdırılması, web sayfasının ele geçirilmesi gibi saldırı senaryoları karşısında kurumların verdiği tepkiler yazılı olarak değerlendirildi.

Ulusal Siber Güvenlik Tatbikatı 2012'nin TÜBİTAK BİLGEM ve BTK koordinatörlüğünde Aralık 2012'de yapılacağı duyuruldu.

Ayrıca BTK tarafından 8-29 Mayıs 2012 tarihleri arasında internet servis sağlayıcılara gelebilecek tehditleri göstermek için, on iki internet servis sağlayıcının katılımıyla Siber Kalkan Tatbikatı 2012 gerçekleştirildi.

Siber suçlar üzerine yapılan çalışmalar

Türkiye'de 35 milyonu aşkın internet kullanıcısı olması özellikle de "sosyal ağ" denilen Facebook, Twitter, Linkedin, YouTube gibi sitelerin kullanımını da artırdı. Sosyal ağlardaki Türk kullanıcı sayıları:

31 milyon facebook kullanıcısı
7,5 milyon twitter kullanıcısı
1 milyon linkedin kullanıcısı

Kullanıcıların % 25'i internetsiz yaşayamayacaklarını, % 41'i her gün internete girdiğini, % 33'ü sosyal medya sitelerine girmedikleri takdirde arkadaşları ile bağlarının kopmasından korktuğunu belirtiyor. Bu durum, siber tehditlerin hedef alanlarından birinin de sosyal ağlar olmasını sağlamıştır. Norton Siber Suçlar 2012 verilerine göre Türkiye'de en az 10 milyon kişi siber suçlara maruz kalmış, bu suçların toplam maliyeti 1 milyar TL olarak tespit edilmiştir. Kullanıcıların genellikle kolay tahmin edilen parola kullanması (ki bu oran % 29) hesaplarının çalınmasına yol açıyor.

Türkiye'deki internet kullanıcılarının bilgi güvenliği/siber güvenlik farkındalığının artırılması amacı ile TÜBİTAK BİLGEM tarafından Bilgimi Koruyorum E-Öğrenme Projesi http://www.bilgimikoruyorum.org.tr adlı bir site kuruldu. Site, kullanıcılara sadece kendilerini korumayı öğretmeyi değil, onları siber saldırılara alet olmamak konusunda bilinçlendirmeyi de amaçlıyor.

Ayrıca Siber Güvenlik Derneği, Bilgi Güvenliği Derneği gibi sivil toplum kuruluşları düzenledikleri konferanslar, seminerler ve eğitimler ile toplumda siber güvenlik farkındalığı oluşturuyor.

Son yıllarda özellikle protesto amaçlı "hacktivizm" faaliyetlerinden büyük kamu kurumları ve özel şirketler de nasibini alıyor. Özellikle servis dışı bırakma, web sayfası içeriği değiştirme gibi saldırılara maruz kalan kurumların verdiği hizmetler sekteye uğruyor. Servis dışı bırakma saldırıları sırasında saldırının etkisinin uzun sürmesi, saldırganların hiçbir bilgi birikimi olmasa da kolaylıkla yapılabilmelerinden ve saldırıya uğrayan kurumun diğer kurumlarla arasındaki koordinasyon eksikliğinden kaynaklanıyor.

Siber suçlara karşı uluslararası düzeydeki ilk sözleşme Avrupa Konseyi tarafından hazırlanan Siber Suç Sözleşmesi'dir. Sözleşmeyi otuz dokuz Avrupa Konseyi üyesi, ABD, Kanada, Japonya ve Güney Afrika olmak üzere toplam kırk üç ülke imzaladı. Türkiye de 10 Kasım 2010'da Dışişleri Bakanlığı düzeyinde bu belgeyi imzaladı. Sözleşme, TBMM'nin onayından sonra yürürlüğe girecek ve internet konusundaki tüm mevzuat bu sözleşme hükümlerine göre yeniden düzenlenecek.

Stuxnet, flame gibi zararlı yazılımlar vasıtasıyla örneği görülen Gelişmiş Siber Casusluk Tehdidi (*Advanced Persistent Threat)* saldırıları ise enerji sistemleri gibi kritik altyapıları hedef alarak ülkelerin güvenliğini siber casusluk ve siber sabotaj ile tehdit ediyor.

Ülkemiz için henüz bir siber güvenlik stratejisi belirlenmemiştir. Fakat 20 Ekim 2012 tarihli Milli Güvenlik Kurulu kararı ile siber güvenlikle ilgili olarak alınacak önlemleri belirlemek ve bunların uy-

gulanmasını ve koordinasyonunu sağlamak amacıyla Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın başkanlığında Siber Güvenlik Kurulu kurulmuş, böylece siber güvenliğin devlet seviyesinde ele alınmasına imkân sağlanmıştır. Ayrıca "siber terör" kavramı Genelkurmay Başkanlığı'nın önerisi ile Milli Güvenlik Siyaset Belgesi'ne eklenmiştir.

2012 Temmuz'unda TÜBİTAK BİLGEM'e bağlı Siber Güvenlik Enstitü'nün açılması, siber güvenlik alanında daha etkin ARGE yapılmasına olanak sağlamıştır. Üniversitelerde de siber güvenlik üzerine akademik çalışmaların, lisansüstü ve doktora düzeyinde yapılması için Yaşar Üniversitesi'nde Siber Güvenlik Bilim Dalı açılmıştır; önümüzdeki süreçte daha çok üniversitede siber güvenlik bilim dalı açılacağına dair bilgiler de var. Yine siber güvenlik uzman açığının kapatılması için 2012 Temmuz'unda elli üniversite öğrencisinin siber güvenlik alanında eğitilmesi amacıyla TÜBİTAK BİLGEM ve Bilgi Güvenliği Akademisi tarafından Siber Güvenlik Yaz Kampı düzenlenmiş ve bu tür etkinliklerin her sene yapılması ve daha fazla öğrencinin yetiştirilmesi kararlaştırılmıştır.

Siber Savaş hukuku

Savaş "bir toplumun, bir ulusun veya devletler topluluğunun kendi isteklerini, başka bir ulus ve devletler topluluğuna zorla kabul ettirmek amacıyla giriştiği mücadele" şeklinde tanımlanıyor. Savaşların adil olması, öncesinde ve sonrasında sivillere ve kamu mallarına verilecek zararların en aza indirilmesi için işin hukuksal yönünün de oluşturulması gerekiyor. Savaş hukuku, savaşan ülkelerin birbirleriyle ve savaşa katılmayan ülkelerle olan ilişkilerini düzenler, ayrıca bireylerin savaştaki hak ve sorumluluklarını belirtir. Savaş hukuku ile savaş sebebiyle yapılması gereken askeri eylemlerin ve insancıl gereklerin bağdaştırılmasına çalışılır. Savaş hukukunun amacı, savaşın sebep olduğu vahşeti olabildiğince azaltmaktır.

Siber uzayın sınırlarının olmaması, siber savaşlarda saldırının nereden geldiğinin belirlenmesini de hayli karmaşık bir iş haline getiriyor. Örneğin siber savaşlarda, saldırı düzenleyen ülkenin saldıracağı ülkeyle sınırı olması gerekmiyor. "Köle" bilgisayarların kullanılması ile başka ülkeler üzerinden saldırı gerçekleştirmek ya da fiziksel olarak bir başka ülkenin internet hatlarının kullanılması ve bunun üçüncü bir ülkeye sorumluluk getirmesi gibi konular, siber savaşların hukukunu hayli karmaşık hale getiriyor. Eğer bir devlet başka bir devletin finans, elektrik dağıtım, doğalgaz, baraj, trafik sinyalizasyon gibi sistemlerini hedef alıyorsa, bu savaştan çok teröre giriyor. Savaşların haklı nedenleri olabilir, fakat terörün haklı nedeni yoktur. Bu nedenle, yapılacak uluslararası hukuki çalışmalarla, gelişen ve büyüyen siber savaş ortamının çerçevesinin bir an önce tanımlanması ve ülkelerin bu çerçeveyi bir antlaşma ile kabul etmesi gerekiyor.

Sonuç

"3. Dünya Savaşı'nda hangi silahların kullanılacağını bilmiyorum, ama 4. Dünya Savaşı'nda taş ve sopalar olacağını biliyorum". Tüm zamanların en parlak ve en tanınmış fizikçisi Albert Einstein'a ait olan bu söz, insanlığın neredeyse tamamını yok edecek güçte silahlar üretilebileceğini, dolayısıyla bir sonraki savaşı yapmak için Dünya'da insan kalmayabileceğini ifade eder. Fakat bu söz, savaş gerçeğini yok edemiyor. Farklı bir boyutta yapılıyor olsa da, savaşa hazırlık her zaman önemli.

2023 yılına kadar en az üç nükleer enerji santrali inşa etmek isteyen Türkiye'nin stuxnet/flame/duqu benzeri siber saldırılara hedef olmamak için gerekli siber savunma altyapısını kurması ve hazırlıklarını yapması gerekiyor.

Siber savaşta etkin savunma yapılabilmesi için siber güvenlik konusunun iyi kavranması gerekiyor. Bu bağlamda yasal düzenlemelerin yapılması, uluslararası hukuktan kaynaklanan hakların kullanılabilmesi için hazırlık yapılması, ulusal bilgisayar olaylarına müdahale organizasyonunun oluşturulması, ulusal siber güvenlik altyapısının güçlendirilmesi, siber güvenlik alanında insan kaynağı yetiştirilmesi, siber güvenlikte milli teknolojilerin geliştirilmesi için seferber olunması gerekiyor.

Kaynaklar
www.bilgiguvenligi.gov.tr
www.bilgimikoruyorum.org.tr
http://portal.ubap.org.tr/App_Themes/Dergi/2008-79-470.pdf>
http://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf
Hildreth, S. A., "Cyberwarfare Congressional Research Service Report for Congress", Congressional Research Service & The Library of Congress, No: RL30375, 2001.
http://tr.wikiquote.org/wiki/Albert_Einstein