2blackdot

“Esasen konu hep 2 nokta arasındadır”

Haftalık
Politik ve Jeopolitik
Gelişmeler

02 Haziran 2025

TEMA GRUP

Bu hizmet size **2blackdot** ve **Tema Grup** tarafından ücretsiz verilmektedir. **Bu yazılanlar yatırım tavsiyesi değildir.**

Hazırlayan: Hakan Çalışkantürk **2twoblackdots@gmail.com** **https://www.2blackdots.com**

21. YÜZYILIN YENİ CEPHESİ: SİBER GÜVENLİĞİN KÜRESEL ÖNEMİ VE SİBER SAVAŞLAR

Prof. Dr. Murat KOÇ

Özet

Günümüz dünyasında uluslararası çatışmaların ve güvenlik dinamiklerinin önemli bir boyutu dijital ortama taşınmıştır. Siber güvenlik, yalnızca teknik bir mesele olmaktan çıkmış, küresel ekonomiden ulusal güvenliğe kadar geniş bir yelpazede kritik bir unsur haline gelmiştir. Bu çalışma, siber savaşların küresel önemi ile özellikle ekonomik etkilerine odaklanmaktadır. Estonya'ya 2007'de düzenlenen siber saldırı, Stuxnet (2010) virüsü, WannaCry (2017) fidye yazılımı, SolarWinds tedarik zinciri saldırısı (2020) ve devam eden Ukrayna-Rusya savaşı gibi olaylar ışığında, siber savaşların dünya ekonomisine verdiği zararlar ve toplumsal hayatı nasıl sekteye uğratabileceği incelenmektedir. Ayrıca Rusya ve Çin'in artan siber gücü ile bu güçlerini nasıl stratejik birer silah olarak kullandıkları irdelenmekte, bunun ekonomik ve siyasi sonuçları tartışılmaktadır. Makale, savaş olgusunun değişen doğasını ele alarak fiziksel cephelerden dijital ve hibrit savaşlara geçişi, siber savaşların karakteristik özelliklerini ve gelecekte ortaya çıkabilecek tehditleri analiz etmektedir. Teknoloji, finans, altyapı ve enerji gibi kritik sektörlere yönelik siber saldırı örnekleri üzerinden, siber savaşların ekonomik etkileri somut bir biçimde ortaya konmaktadır. Bu kapsamlı bakış açısı ile çalışma, 21. yüzyılın "yeni cephesi" olan siber uzayın, küresel güvenlik ve istikrar açısından neden merkezi bir öneme sahip olduğunu vurgulamaktadır.

Giriş

Dijital teknolojilerin hayatın her alanına nüfuz ettiği 21. yüzyılda, uluslararası güvenlik ve çatışma kavramları da köklü bir değişim geçirmektedir. Bir zamanlar yalnızca bilimkurgu senaryolarında rastlanabilecek siber savaşlar, günümüzde devletlerin ve devlet dışı aktörlerin sıklıkla başvurduğu bir mücadele yöntemi haline gelmiştir. Kritik altyapıların dijitalleşmesi, ekonomilerin ağlar üzerinden işlemesi ve toplumların çevrimiçi platformlara bağımlı hale gelmesi, siber uzayı adeta yeni bir savaş alanı konumuna getirmektedir. Artık hemen her büyük ölçekli çatışmada dijital cephede de bir mücadele sürmekte; başka bir deyişle her savaşın bir siber boyutu bulunmaktadır.

Bu gerçek, siber güvenliğin küresel ölçekte hayati önem kazanmasına yol açmıştır. Siber saldırılar, fiziksel bir savaş ilan edilmeksizin ülkelerin finans sistemlerini, elektrik şebekelerini, iletişim altyapılarını ve hatta seçim süreçlerini hedef alabilmektedir. Üstelik bu saldırılar coğrafi sınırlara tabi değildir; bir ülkede geliştirilen zararlı bir yazılım, küresel ölçekte domino etkisiyle milyonlarca sistemi etkileyebilir. Devlet destekli gruplar veya organize suç şebekeleri tarafından yürütülen siber operasyonlar, küresel ekonomiye milyarlarca dolarlık zararlar verebilmektedir.

Bu durum, siber uzayı ulusal güvenlik kadar ekonomik refahın da mücadele edildiği bir cephe haline getirmektedir. Bu makalede, siber savaşların neden küresel ölçekte kritik bir mesele haline geldiği çok boyutlu olarak incelenecektir. İlk olarak, yakın tarihte dünya gündemini sarsan büyük siber saldırı örnekleri üzerinden siber savaşların küresel ekonomi üzerindeki etkileri ele alınacaktır. Ardından, Rusya ve Çin'in siber uzaydaki yükselen gücü ve uyguladıkları stratejiler analiz edilecek; bu güç projeksiyonunun ekonomik ve siyasi sonuçları tartışılacaktır. Makale, savaşın değişen doğasını irdeleyerek, geleneksel konvansiyonel çatışmalardan dijital/hibrit savaş konseptine geçişi ve siber savaşların kendine özgü özelliklerini ortaya koyacaktır. Son olarak, teknoloji, finans, altyapı ve enerji gibi farklı sektörlerde siber savaşların doğurduğu ekonomik etkiler örneklerle açıklanacak ve genel bir değerlendirme ile sonuçlandırılacaktır.

Siber Savaşların Küresel Ekonomi Üzerindeki Etkileri

Siber saldırıların ekonomik bedeli, hem hedef alınan ülke ve kurumlar hem de küresel ekonomi açısından ciddi boyutlara ulaşabilmektedir. Tarihteki ilk büyük çaplı devlet ölçekli siber saldırı örneklerinden biri sayılan Estonya 2007 vakası, ekonomik etkileriyle bu duruma çarpıcı bir örnek oluşturur. Nisan-Mayıs 2007'de Estonya'ya yönelik gerçekleştirilen yoğun DDoS (dağıtık hizmet dışı bırakma) saldırıları sonucunda ülkenin bankacılık sistemi, devlet daireleri ve medya kuruluşları günlerce işlevsiz kalmıştır. Küçük bir Baltık ülkesi olan Estonya, dijital altyapıya en bağımlı ülkelerden biri olduğu için saldırının etkisini derinden hissetmiştir. Yapılan analizler, bu siber saldırıların Estonya'ya kısa vadede yaklaşık 750 milyon ABD doları tutarında bir ekonomik kayba mal olduğunu ortaya koymuştur.

Nitekim Estonya'nın GSMH'si ile kıyaslandığında bu tutar ciddi bir orana denk gelmektedir ve hükümet hizmetlerinin aksaması, bankacılık işlemlerinin durma noktasına gelmesi gibi sonuçlar doğurmuştur. Estonya örneği, siber saldırıların sadece hedef ülkenin ekonomisini sarsmakla kalmayıp uluslararası yankılar uyandırdığını göstermiştir; zira bu olay NATO'yu da alarma geçirmiş ve İttifak, Tallinn'de NATO Kooperatif Siber Savunma Mükemmeliyet Merkezi'ni (CCDCOE) kurarak siber savunmaya odaklanmaya başlamıştır.

2010 yılında ortaya çıkan Stuxnet saldırısı, siber savaşların ekonomik ve stratejik etkisine dair farklı bir boyut sunmaktadır. Stuxnet, muhtemelen ABD ve İsrail tarafından İran'ın nükleer programını sabote etmek amacıyla geliştirilen bir bilgisayar solucanı olarak tarihe geçmiştir. Bu zararlı yazılım, İran'ın Natanz nükleer tesisindeki santrifüjleri hedef alarak onların denetim sistemlerini bozmuş ve fiziksel hasara yol açmıştır. Sonuçta İran, kısa süre içinde yaklaşık 1.000 uranyum zenginleştirme santrifüjünü devre dışı bırakıp yenilemek zorunda kalmıştır.

Bu, İran'ın nükleer programını yavaşlatmış olmanın yanı sıra ekonomik olarak da ülkeye ek bir maliyet getirmiş ve uluslararası enerji piyasalarında belirsizlik yaratmıştır. Stuxnet vakası, siber saldırıların sadece dijital dünyayla sınırlı kalmayıp fiziksel dünyada da yıkıcı sonuçlar doğurabileceğini gösteren ilk somut örneklerden biri olmuştur. Böylece siber uzayın, devletlerin stratejik çıkarlarına ulaşmak için kullanabileceği etkili bir saldırı alanı haline geldiği anlaşılmıştır.

WannaCry fidye yazılımı salgını

WannaCry (2017) fidye yazılımı salgını, küresel ekonomiye zarar veren siber saldırılara bir diğer önemli örnektir. Mayıs 2017'de başlayıp hızlıca dünya geneline yayılan WannaCry, aralarında Britanya'daki Ulusal Sağlık Servisi (NHS) hastaneleri, İspanya'daki telekom şirketi Telefónica ve birçok ülkenin kritik kurumlarının bulunduğu on binlerce sistemi etkiledi. Eski veya yamalanmamış Windows sistemlerindeki bir güvenlik açığından yararlanan bu zararlı, önemli dosyaları şifreleyip kullanılmaz hale getirdi ve kullanıcılarından fidye talep etti. WannaCry saldırısının 150 ülkede 300 binden fazla bilgisayarı etkilediği tahmin edilmektedir.

Küresel ölçekte bakıldığında, bu saldırı sonucu oluşan hasarın ve faaliyet kesintilerinin toplam maliyetinin 4 milyar ABD dolarına kadar ulaştığı hesaplanmıştır. Sadece İngiltere'de sağlık sistemine verdiği zarar 90 milyon sterlini bulmuştur. WannaCry olayı, siber saldırıların finansal etkilerinin ne denli geniş alanlara yayılabileceğini göstermiş; bir ülkedeki zayıflığın küresel çapta şirketleri ve kamu hizmetlerini aksatabileceğini ortaya koymuştur.

Not Petya saldırısı

Yine 2017 yılının Haziran ayında meydana gelen NotPetya saldırısı ise, tarihin en maliyetli siber vakalarından biri olarak anılmaktadır. Ukrayna'ya yönelik bir siber savaş hamlesi olarak başlayan NotPetya adlı yıkıcı malware (zararlı yazılım), kısa sürede sınırları aşıp dünya genelinde birçok büyük şirketi felç etmiştir. Başlangıç noktası Ukrayna'daki yaygın bir muhasebe yazılımının güncelleme mekanizmasına sızılması olan bu saldırı, fidye yazılım süsü verilmiş bir veri silme saldırısıdır. Sonucunda Danimarkalı nakliye devi Maersk, ABD'li ilaç şirketi Merck, FedEx gibi küresel şirketler ciddi operasyonel kesintilere uğramış, Ukrayna'da ise banka ve enerji şirketleri durma noktasına gelmiştir. Bu saldırının küresel ölçekte yol açtığı toplam zararın 10 milyar ABD doları civarında olduğu tahmin edilmektedir.

NotPetya, bir devlet destekli siber saldırının (muhtemelen Rusya'nın askeri istihbarat servisi GRU tarafından) kontrolden çıkıp dünya ekonomisinde milyarlarca dolarlık hasar yaratabileceğine çarpıcı bir örnek teşkil etmiştir. Nitekim bu olay sonrasında siber risklere karşı sigorta sektörünün de temellerinden sarsıldığı ve şirketlerin siber güvenlik yatırımlarını artırdığı gözlenmiştir

SolarWinds siber casusluk kampanyası

Daha yakın tarihte, Aralık 2020'de ortaya çıkarılan SolarWinds siber casusluk kampanyası, siber saldırıların karmaşık tedarik zinciri üzerinden gerçekleştirilip küresel ölçekte etki yaratabileceğini gösterdi. SolarWinds şirketinin Orion adlı ağ yönetim yazılımına sızan saldırganlar (ileri düzeyde bir tehdit aktörü, büyük olasılıkla Rusya'nın dış istihbarat servisi SVR), bu yazılımın güncelleme mekanizmasına zararlı kod enjekte ederek SolarWinds müşterilerinin sistemlerine arka kapı yerleştirdiler. Bu yöntemin sonucunda ABD'de Dışişleri, Hazine, İç Güvenlik, Adalet Bakanlıkları gibi kritik devlet kurumları ile yüzlerce büyük şirket etkilendi. Saldırının doğrudan bir sistem yıkımına yol açmaması nedeniyle ekonomik etkisi ilk bakışta belirsiz olsa da, on binlerce sistemin temizlenmesi, ağların yeniden güvenceye alınması ve hasarın tespiti için harcanan kaynaklar muazzam boyutlara ulaştı. Uzmanlar, SolarWinds gibi bir tedarik zinciri saldırısının etkilerini tamamen gidermek ve ağ güvenliğini tekrar sağlamak için küresel çapta harcanacak bütçenin 100 milyar dolara kadar çıkabileceğini öngörmüştür.

Bu olay, siber casusluk operasyonlarının bile şirket hissedarlarından devlet hazinelerine kadar ekonomik maliyet doğurabileceğini ve güvenlik yatırımlarını artırma zorunluluğu getirdiğini göstermiştir. Son olarak, Rusya ile Ukrayna arasındaki savaş (2014'ten bu yana devam eden ve 2022'de geniş çaplı işgale dönüşen çatışma) siber savaşlar ile fiziksel savaşların iç içe geçtiği ve ekonomilere büyük yansıma yaptığı bir durumdur. Rusya, Ukrayna'ya karşı tanklar ve füzelerle yürüttüğü savaşın yanında, uzun yıllardır Ukrayna'nın elektrik şebekesini, finans sistemini ve medya altyapısını hedef alan sayısız siber operasyon gerçekleştirmiştir.

Örneğin, 2015 ve 2016 yıllarında Ukrayna'nın elektrik dağıtım şebekesine düzenlenen saldırılar sonucunda Kiev başta olmak üzere bazı bölgelerde saatlerce elektrik kesintileri yaşanmıştır. 2022'deki geniş çaplı işgalin hemen öncesinde ve sonrasında, Ukrayna'ya yönelik siber saldırılarda belirgin bir artış gözlenmiştir. Ukrayna Siber Güvenlik Ajansı'nın raporlarına göre, 2024 yılı içinde Ukrayna'ya yönelik Rus kaynaklı siber saldırıların sayısı bir önceki yıla kıyasla yaklaşık %70 artmış ve kritik altyapıya yönelik 4.315 vakaya ulaşmıştır. Bu saldırılar devlet kurumlarını, enerji

sektörünü ve savunma ile ilgili kuruluşları hedef almış; amaçları arasında hassas verileri çalmak ve operasyonları aksatmak yer almıştır.

Rusya'nın Ukrayna'ya karşı gerçekleştirdiği bu dijital taarruzlar, sadece Ukrayna ekonomisini yıpratmakla kalmamış, aynı zamanda 2017'deki NotPetya örneğinde olduğu gibi küresel tedarik zincirlerini ve piyasa güvenini de etkilemiştir. Dahası, Ukrayna'ya saldırmak için kullanılan bazı zararlı yazılımlar kontrolsüz biçimde diğer ülkelere yayılabilmekte, bu da uluslararası iş dünyasında operasyonel maliyetlere ve güvenlik harcamalarına yansımaktadır. Yukarıdaki örnekler, siber savaşların küresel ekonomi üzerinde çok yönlü ve ciddi etkileri olabileceğini açıkça ortaya koymaktadır. Bankacılık sistemlerinin çökmesi, fabrikaların üretimi durdurması, hastanelerin hizmet veremez hale gelmesi veya enerjinin kesilmesi gibi sonuçlar, doğrudan finansal kayıpların ötesinde güven kaybına ve belirsizliğe yol açarak piyasalarda dalgalanmalara neden olmaktadır. Bu nedenle, siber güvenlik artık yalnızca teknik bir konu değil, ekonomik istikrarın ve ulusal güvenliğin temel bir bileşeni olarak değerlendirilmektedir.

Rusya'nın ve Çin'in Artan Siber Gücü ve Stratejileri

Rusya: Saldırı Odaklı Hibrit Siber Stratejiler

Rusya Federasyonu, son on yılda gerçekleştirdiği yüksek profilli siber operasyonlarla bu alandaki en etkin aktörlerden biri haline gelmiştir. Rus doktrininde "siber" kavramı, salt teknik saldırılarla sınırlı görülmemekte, bilgi savaşı kavramı altında psikolojik operasyonlarla iç içe geçmiş bir bütün olarak ele alınmaktadır. Nitekim Rusya, teknik siber saldırılar (ağlara sızma, zararlı yazılım, DDoS vb.) ile psikolojik ve dezenformasyon operasyonlarını ayrılmaz bir şekilde görmektedir.

Bu stratejik yaklaşım, Kremlin'in siber alandaki hamlelerine geniş bir manevra alanı sağlamaktadır: Bir yandan elektrik şebekeleri veya devlet daireleri gibi kritik altyapıları hedef alırken, diğer yandan sosyal medya ve propaganda yoluyla kamuoyunu etkilemeye çalışmaktadır. Rusya'nın askeri istihbarat servisi GRU başta olmak üzere çeşitli devlet kurumlarıyla bağlantılı hacker grupları, dünya genelinde pek çok saldırının faili olarak görülmektedir. Yapılan araştırmalar, Rus askeri istihbaratına bağlı siber operasyonların son on yılda düzinelerce ülkede seçimleri baltaladığını, ekonomilere zarar verdiğini ve insanları tehlikeye attığını ortaya koymaktadır.

Örneğin GRU bağlantılı olduğundan şüphelenilen Sandworm veya APT28 gibi gruplar, 2015 ve 2016'da Ukrayna'nın elektrik şebekesini iki kez çökertmiş; 2017'de NotPetya adlı veri silici yazılımı küresel çapta serbest bırakarak çok sayıda şirketi zarara uğratmıştır.

Yine Rus kaynaklı hackerlar, Dünya Anti-Doping Ajansı (WADA), çeşitli gazeteciler ve siyasetçiler hakkında gizli bilgileri sızdırarak itibarsızlaştırma kampanyaları yürütmüş, 2016 ABD başkanlık seçimlerinde Demokratik Parti e-postalarının sızdırılması gibi operasyonlarla siyasi süreçlere müdahil olmuşlardır. Tüm bu faaliyetler, Rusya'nın hibrit savaş konseptinin bir parçası olarak siber gücünü hem askeri hem siyasi hedeflerine ulaşmak için kullandığını göstermektedir. Rusya'nın siber stratejileri incelendiğinde, birkaç temel motivasyon öne çıkmaktadır: istihbarat toplama, stratejik sabotaj ve etki operasyonları. İstihbarat amaçlı olarak Rus devlet destekli gruplar, rakip gördükleri ülkelerin devlet kurumlarına, savunma sanayi şirketlerine ve diplomatik ağlarına sızarak gizli bilgiler toplamaktalar. Örneğin 2020'de ortaya çıkan SolarWinds saldırısı, büyük ölçüde ABD'li kurumların e-postalarını ve gizli verilerini uzun süre fark edilmeden izlemeye yönelik bir istihbarat operasyonuydu. Stratejik sabotaj boyutunda ise Rusya, özellikle yakın coğrafyasındaki ülkelerin kritik altyapılarına zarar vermeyi hedefleyen siber silahlar kullanmıştır; Ukrayna'nın enerji altyapısına yönelik saldırılar ve Gürcistan'a 2008'deki askeri harekâtla eşzamanlı yapılan siber saldırılar bu kapsamda değerlendirilebilir. Etki operasyonları açısından bakıldığında ise Rusya, sosyal medya ve hack-sızdır taktiklerini birleştirerek dış politik hedeflerine uygun şekilde toplumların algısını etkilemeye çalışmaktadır. Bu, "Gerçeklerin bulanıklaştırılması" olarak da adlandırılan ve Rusya'nın dezenformasyonla siber saldırıyı koordineli kullandığı sofistike bir yöntemdir. Rusya'nın siber alandaki kabiliyetleri ve saldırgan tutumu, ekonomik ve siyasi sonuçlar da doğurmaktadır. Ekonomik açıdan Rusya kaynaklı siber tehditler, hedef ülkelerde siber güvenlik harcamalarının ve sigorta maliyetlerinin artmasına yol açmakta; örneğin NotPetya sonrası küresel şirketler milyarlarca doları sistem yedekleme ve ağ segmentasyonu gibi önlemlere yatırmak zorunda kalmıştır. Siyasi açıdan ise Rusya'nın bu faaliyetleri uluslararası arenada gerginliklere ve yaptırımlara neden olmuştur. Birçok ülke, vatandaşlarına veya altyapılarına yönelik siber saldırılar nedeniyle Rusya'yı açıkça suçlamış; ABD ve Avrupa Birliği gibi aktörler, Rus yetkililere ve şirketlere siber saldırılar dolayısıyla yaptırımlar uygulamıştır. Öte yandan, siber saldırıların inkâr edilebilir doğası (failin gizlenebilmesi) Rusya'nın bu operasyonları çoğunlukla resmi sorumluluk üstlenmeksizin yapmasına imkân tanımaktadır. Bu da uluslararası hukuk ve caydırıcılık mekanizmaları açısından yeni bir meydan okuma yaratmaktadır.

Çin: Siber Casusluk ve Uzun Vadeli Avantaj Stratejileri

Çin Halk Cumhuriyeti, siber uzayı ekonomik ve askeri yükselişinin bir aracı olarak kullanan bir diğer süper güçtür. Çin'in siber stratejileri, Rusya'nın aksine daha ziyade düşük profilli, uzun vadeli kazançlara odaklanır görünmektedir. Özellikle siber casusluk (siber espionaj) ve fikri mülkiyet hırsızlığı, Çin kaynaklı siber faaliyetlerin

odak noktasını oluşturmaktadır. ABD Federal Soruşturma Bürosu (FBI) tarafından hazırlanan bir rapora göre, sahte ürünler, korsan yazılımlar ve ticari sır hırsızlığı yoluyla ABD ekonomisine yılda 225 ile 600 milyar dolar arasında zarar verildiği ve bu konuda dünyanın en büyük faillerinin başında Çin'in geldiği belirtilmektedir.

Bu çarpıcı rakam, Çin'in siber uzaydaki faaliyetlerinin ekonomik motivasyonunu gözler önüne sermektedir. Çinli hacker grupları, devlet desteğiyle, yabancı şirketlerin Ar-Ge sırlarını, ileri teknolojilerini ve ticari avantaj sağlayacak bilgilerini sistematik biçimde çalmaktadır. Bu sayede Çin, kendi sanayisini ve teknolojik gelişimini hızlandırırken, rakip ekonomilerin rekabet avantajını azaltmayı hedeflemektedir. Çin'in siber kabiliyetleri yalnızca ekonomik casusluk ile sınırlı değildir. Halk Kurtuluş Ordusu (PLA) bünyesinde kurulan Stratejik Destek Kuvvetleri (Strategic Support Force) gibi yapılanmalarla Çin, askeri olarak da siber uzaya büyük yatırım yapmaktadır. Çinli siber aktörler, tıpkı Rusya gibi, rakip olarak gördükleri ülkelerin kritik altyapılarına sızma ve gerekirse sabotaj yapma kapasitesine sahiptir. Ancak Çin'in bu alandaki yaklaşımı, genellikle "savaş eşiğinin altında" kalacak düzeyde, daha örtülü operasyonlar şeklindedir.

Yani Çin, siber araçları kullanarak doğrudan bir savaş nedeni (casus belli) sayılmayacak, ancak stratejik avantaj sağlayacak hamleler yapmaya özen göstermektedir. Örneğin 2015 yılında ABD'de Federal Personel Yönetimi Ofisi (OPM) veri tabanına sızılarak 21,5 milyon federal çalışanın kişisel verilerinin çalınması hadisesi, Çin'e atfedilen büyük bir siber casusluk operasyonudur.

Bu saldırı, Çin'in rakip gördüğü bir ülkenin devlet personeline ait ayrıntılı güvenlik soruşturması bilgilerini ele geçirerek istihbarat oluşturma amacına işaret etmektedir. Çin, aynı zamanda askeri bir çatışma durumunda rakiplerini baskılamak için de siber saldırı kozunu elde tutmaktadır. Özellikle Doğu Asya'da artan jeopolitik gerilim (örneğin Tayvan meselesi) bağlamında, Çin'in ABD'yi bölgeden caydırmak için siber saldırı tehditlerini kullandığı ifade edilmektedir. Nitekim bir rapora göre Çin, savaş eşiğinin altında kalacak şekilde siber saldırılarla rakiplerini yıldırma stratejisi izlemekte; örneğin ABD'nin Asya'daki varlığını caydırmak amacıyla Amerikan kritik altyapılarını hedef almaktadır.

Bu tür saldırılar, karşı tarafa "eğer müdahil olursan kendi altyapın da risk altında" mesajı vermeyi amaçlayan caydırıcı hamlelerdir. Çin'in siber gücünün ekonomik ve siyasi sonuçları da dikkat çekicidir. Ekonomik olarak, Çin kaynaklı siber hırsızlıklar bir yandan Çin'in teknolojik ilerlemesini hızlandırırken, diğer yandan hedef ülkelerde büyük ekonomik kayıplara yol açmaktadır. Örneğin çalınan fikri mülkiyetin piyasa değeri, ilgili şirketler ve ekonomiler için uzun vadede ciddi zararlar demektir. ABD'li yetkililer, Çin'in siber casusluk faaliyetlerinin Amerikan ekonomisine verdiği zararı "tarihteki en büyük servet transferi" olarak nitelendirmiştir. Bunun sonucu olarak ABD ile Çin arasında teknoloji transferi, ticari sırların korunması ve siber casusluk konularında yüksek tansiyonlu diplomatik tartışmalar yaşanmaktadır. Çinli askeri hackerların açığa çıkarılması, ABD Adalet Bakanlığı tarafından Çin'li ajanlar hakkında iddianameler hazırlanması ve iki ülkenin birbirine karşı siber uzayda suçlamaları, yeni bir siber Soğuk Savaş atmosferi oluşturmuştur. Siyasi boyutta ise Çin, siber uzaydaki gücünü sadece saldırı değil, kontrol ve sansür amacıyla da kullanmaktadır. Ülke içinde "Büyük Güvenlik Duvarı" (Great Firewall) ile interneti denetim altında tutan Pekin yönetimi, dışarıya karşı da kendi çıkarlarına aykırı bilgi akışını engellemeye, diaspora hareketlerini izlemeye yönelik siber operasyonlar yürütmektedir. Ayrıca son dönemde Çin'in propaganda ve etki operasyonlarına siber unsurları kattığı, örneğin sosyal medya platformlarında dezenformasyon kampanyaları yürüttüğü görülmektedir (Kanada'da WeChat uygulaması üzerinden bir siyasi figüre karşı yürütülen karalama kampanyası buna örnek verilebilir).

Özetle, Rusya ve Çin günümüzün iki büyük siber süper gücü olarak farklı taktik ve hedeflerle de olsa ABD gibi dijital cepheyi yoğun biçimde kullanmaktadır. Rusya daha saldırgan, kaos çıkarmaya yönelik ve politik-askeri kazanımlara odaklı siber operasyonlarla öne çıkarken; Çin daha gizli, uzun vadede ekonomik ve stratejik avantaj sağlamaya dönük siber casusluk faaliyetleriyle dikkat çekmektedir. Her iki ülkenin eylemleri de uluslararası güvenlik mimarisini zorlamakta, siber alanda yeni normlar ve caydırıcılık yöntemleri geliştirilmesini zorunlu kılmaktadır.

Savaşın Değişen Doğası: Fiziksel Cepheden Dijital/Hibrit Cepheye

Tarih boyunca savaş kavramı, teknoloji ve toplum yapılarındaki değişimlere paralel olarak evrim geçirmiştir. Tarım toplumlarının kılıç kalkan muharebelerinden sanayi devrimi sonrası topyekûn savaşlara, nükleer çağın stratejik dengelerinden günümüzün dijital çatışmalarına kadar, savaşın doğası sürekli bir dönüşüm içindedir. 21. yüzyıla gelindiğinde ise savaşın doğasında belki de en radikal değişim, fiziksel ve dijital cephelerin iç içe geçmesi şeklinde karşımıza çıkmaktadır. Artık savaşlar, sadece karada, denizde veya havada değil; siber uzayda ve bilgi alanında da eş zamanlı olarak cereyan etmektedir. Bu bölüm, savaşın değişen doğasını kavramsal açıdan ele alarak, siber ve hibrit savaş kavramlarını, bu tür savaşların özelliklerini ve geleceğe yönelik öngörüleri incelemektedir.

Hibrit Savaş ve Dijital Cephe

Hibrit savaş, geleneksel askerî güç kullanımının, gayri nizami harp unsurlarının (terör, isyan, vekil güçler vb.) ve siber saldırılar ile propaganda gibi enformasyon harp yöntemlerinin bir arada kullanıldığı, çok katmanlı savaş

stratejilerine verilen isimdir. Bu kavram, özellikle Rusya'nın 2014'te Kırım'ı ilhakı ve Doğu Ukrayna'daki örtülü operasyonları sonrasında popüler hale gelmiştir. Hibrit savaşta amaç, düşmana tek bir cepheden topyekûn saldırmak yerine, farklı alanlarda eşzamanlı baskı kurarak karar verme süreçlerini felce uğratmak ve direncini kırmaktır. Siber operasyonlar ve dijital propaganda, hibrit savaşın kilit unsurlarıdır; zira konvansiyonel çatışmaların yüksek eşiğine varmadan, düşman altyapısına ve toplum psikolojisine zarar verme imkânı sunarlar. Modern çatışma senaryolarında her askerî harekâtın bir dijital boyutu olduğu görülmektedir.

Örneğin, bir füze saldırısından önce düşmanın hava savunma sistemlerinin siber saldırıyla kör edilmesi, ya da bir kara harekâtına paralel olarak düşman ülkenin haberleşme ağlarının çökertilmesi artık askeri planlamaların parçasıdır. Bu durum, fiziksel ve dijital savaş sınırlarının bulanıklaşması ile sonuçlanmaktadır. Öyle ki NATO gibi savunma ittifakları, 2014 Galler Zirvesi'nden bu yana siber uzaya yapılan saldırıların ciddi sonuçlar doğurması halinde kolektif savunma mekanizmasını (Madde 5) işletilebileceğini duyurmuştur.

Yani bir siber saldırı, eğer üye ülkelerce "silahlı saldırı" seviyesinde görülürse, tıpkı bir füze saldırısı gibi ittifakın toplu karşılık vermesine neden olabilecektir. Bu açıklama bile, siber cephenin artık savaşın merkezi bir parçası olarak tanındığını göstermektedir. Hibrit savaşların bir özelliği de belirsizlik ve inkar edilebilirlik unsurudur. Siber saldırılar anonim gerçekleştirilebildiği, vekil güçler kullanıldığı veya bilgi operasyonları gizli yürütüldüğü için, saldırıya uğrayan taraf failin kim olduğunu belirlemekte zorlanabilir. Bu da hukuki ve siyasi karşılık vermeyi güçleştirmektedir. Rusya'nın "yeşil adamlar" taktiğiyle Kırım'da üniformasız askerler kullanması veya siber saldırıları resmen üstlenmemesi, hibrit stratejinin bilinen örnekleridir. Dijital dünyada da benzer şekilde, devletler zaman zaman siber suç örgütleriyle işbirliği yaparak veya kendi hacker gruplarını vekil olarak kullanarak izlerini örtmeye çalışırlar. Bu hibrit taktikler, geleneksel savaş kuramcısı Clausewitz'in "savaş sisine" (fog of war) dijital bir boyut eklemiştir; belirsizlik, kaos ve sürpriz unsuru dijital cephede stratejik olarak kullanılmaktadır.

Siber Savaşların Özellikleri

Siber savaşları, geleneksel savaş türlerinden ayıran bir dizi kendine özgü özellik bulunmaktadır. Bunları anlamak, siber çatışmaların dinamiklerini kavramak açısından önemlidir:

Asimetrik Yapı: Siber alanda saldırgan ile savunan arasındaki güç dengesi, konvansiyonel savaşlardakinden farklıdır. Küçük bir hacker grubu veya maddi kaynakları sınırlı bir devlet, siber silahlarla çok daha büyük bir güce zarar verebilir. Siber saldırıların maliyeti görece düşük, ancak etkisi çok yüksek olabilir. Bu da siber savaşı asimetrik bir mücadele alanı haline getirir. Örneğin küçük bir ülke veya hatta devletten bağımsız bir hacker kolektifi, gelişmiş bir ülkenin kritik altyapısına sızarak ciddi zarar verebilir. Bu durum, caydırıcılık konseptini zorlaştırır; zira klasik anlamda güç dengesi siber ortamda her zaman geçerli değildir.

Anonimlik ve Atıf Zorluğu: Siber saldırıların kaynağını kesin olarak saptamak (attribution) son derece güçtür. Saldırganlar teknik izlerini gizlemek için çeşitli yöntemler kullanır: Başka ülkelerdeki ele geçirilmiş bilgisayarları zıplama tahtası olarak kullanmak, kimliklerini maskelemek, izleri silmek gibi... Bu nedenle bir saldırıyı kimin yaptığını ispatlamak zaman alıcı ve tartışmalı olabilir. Atıfın belirsizliği, saldırgan devletlere inkar imkânı sağlar ve misilleme yapılmasını hukuken-politik olarak karmaşık hale getirir.

Hız ve Küresel Erişim: Siber saldırılar ışık hızında gerçekleşir ve bir kez başlatıldığında coğrafi olarak yayılmaları an meselesidir. Zararlı bir kod, internet üzerinden saatler hatta dakikalar içinde tüm dünyaya bulaşabilir (WannaCry örneğinde olduğu gibi). Bu, siber çatışmaların tepki verme süresini son derece kısalttığı anlamına gelir. Stratejik karar alıcılar için bu hız, erken uyarı sistemleri ve gerçek zamanlı izleme yeteneklerini hayati hale getirmektedir.

Sivil-Askeri Hedef Ayrımının Bulanıklığı: Geleneksel savaş hukukunda askerî hedefler ve sivil hedefler ayrımı gözetilirdi. Oysa siber savaşta bu ayrım silikleşmiştir. Devletlerin kullandığı birçok altyapı (enerji, iletişim, ulaşım, sağlık) sivillerin de yoğun olarak kullandığı ağlardır. Bir ülkenin elektrik şebekesine yönelik siber saldırı, hastanelerden evlere kadar sivilleri etkileyerek dolaylı can kayıplarına bile neden olabilir (örneğin yoğun bakım ünitelerinin elektriksiz kalması gibi). Dolayısıyla siber savaşlar, sivil toplumun tamamını cephe hattına dönüştürme potansiyeli taşır.

Çarpan Etki ve Zincirleme Sonuçlar: Siber uzayda sistemler birbirine bağlı olduğundan, bir noktadaki saldırı beklenmedik zincirleme etkilere yol açabilir. Özellikle tedarik zinciri saldırılarında veya ortak kullanılan yazılımlardaki açıklar istismar edildiğinde, bir saldırı binlerce kurbanı aynı anda etkileyebilir. SolarWinds örneğinde tek bir yazılım güncellemesine sızılması, 18 bin kuruma sızma imkânı vermişti.

Uluslararası Hukuk ve Normların Belirsizliği: Siber savaşların hukuki çerçevesi henüz tam oturmamıştır. Hangi eşikteki bir siber saldırı "silahlı saldırı" sayılacak, meşru müdafaa hakkı ne zaman doğacaktır, siber silahların kullanımı nasıl denetlenecektir gibi sorular büyük ölçüde gri alandadır. Tallinn El Kitabı gibi gayriresmî çalışmalar bazı yorumlar getirse de devletler arası genel kabul görmüş bağlayıcı kurallar yoktur. Bu da siber alanda bir serbest hareket alanı ve belirsizlik yaratmaktadır.

Geleceğe Yönelik Tehditler ve Öngörüler

Siber savaşların geleceği, teknolojik gelişmeler ve küresel güç mücadeleleriyle şekillenecektir. Uzmanlar, önümüzdeki dönemde birkaç kritik tehdidin ve eğilimin öne çıkacağını tahmin etmektedir:

Yapay Zekâ ve Otomasyon: Yapay zekâ (YZ) teknolojileri, siber güvenlikte hem savunma hem saldırı tarafında devrim yaratma potansiyeline sahiptir. Otomatik saldırı araçları, zafiyetleri insan hızının çok ötesinde tespit edip sömürebilir. Aynı şekilde YZ destekli savunma sistemleri de anomali tespitinde ve saldırıların önlenmesinde kullanılacaktır. Ancak YZ'nin kötüye kullanımı, otonom şekilde yayılan ve hedef seçen "akıllı" zararlı yazılımlar anlamına gelebilir. Gelecekte, savunmanın zaaflarından faydalanmak üzere kendi kendini uyarlayan siber silahlar gündeme gelebilir.

Nesnelerin İnterneti (IoT) ve Fiziksel Sonuçlu Saldırılar: Her geçen gün daha fazla fiziksel cihaz internete bağlanmaktadır (akıllı ev sistemleri, otonom araçlar, endüstriyel kontrol sistemleri vb.). IoT ekosistemindeki güvenlik açıklıkları, saldırganlara fiziki dünyada kaos çıkarma fırsatı verebilir. Örneğin akıllı elektrikli araç filolarının hacklenerek trafiğin altüst edilmesi, akıllı şebekelerin manipüle edilerek geniş çaplı elektrik kesintileri veya fabrika tesislerinde endüstriyel kazaların tetiklenmesi mümkündür. Gelecekte siber saldırılar, can kaybına yol açabilecek derecede fiziksel etkiler doğurabilir ki bu, siber savaş kavramını bambaşka bir ciddiyet düzeyine çıkaracaktır.

Kritik Altyapılara Yönelik Sürekli Tehdit: Önümüzdeki yıllarda da enerji, su, ulaşım, sağlık gibi kritik altyapılar siber savaşta başlıca hedef olmaya devam edecektir. Bu alanlarda daha önce örneği görülmemiş büyük saldırılar yaşanabileceği değerlendirilmektedir. Özellikle elektrik şebekeleri ve enerji terminalleri, bir ulusu dize getirmek için en etkili siber hedeflerdir. Uzmanlar, bir "cyber Pearl Harbor" (baskın niteliğinde yıkıcı bir siber saldırı) riskinden bahsetmektedir. ABD'de 2021'de Colonial Pipeline'a yapılan ve doğu yakasında yakıt arzını günlerce aksatan fidye yazılım saldırısı, bu risklerin bir öncülü olarak görülmüştür. Gelecekte devlet destekli aktörlerin benzer yöntemlerle hasım gördükleri ülkelerin altyapılarına daha büyük ölçekte saldırabileceği endişesi vardır.

Kuantum Teknolojileri: Şu an için teorik düzeyde olan kuantum bilgisayarlar, ileride kriptografik sistemleri çözme kapasitesine ulaştığında, bugünkü siber güvenlik mimarisi kökten sarsılabilir. Mevcut birçok şifreleme metodu, kuantum hesaplama ile hızla aşılabileceğinden, kuantum üstünlüğü elde eden bir devlet siber alanda neredeyse sınırsız bir avantaj yakalayabilir. Bu nedenle ABD, Çin, Rusya gibi güçler kuantum bilişim yarışına da girmiş durumdadır. İlerleyen yıllarda "post-kuantum kriptografi" gibi konular siber güvenliğin gündeminde üst sıralara çıkacaktır.

Uzay ve Uydu Sistemleri: Modern toplumlarda iletişim, navigasyon ve istihbarat büyük ölçüde uydulara ve uzay altyapısına bağımlıdır. Bu sistemler de siber saldırılara karşı savunmasız olabilir. Örneğin 2022'de Rusya'nın, Ukrayna savaşı başlangıcında bir Amerikan uydu internet hizmeti sağlayıcısının (Viasat) modemlerini siber saldırıyla devre dışı bıraktığı rapor edilmiştir. Gelecekte uydu sistemlerine yönelik siber saldırılar, hem askeri operasyonları sekteye uğratma hem de sivil iletişimi felç etme amaçlı kullanılabilir. Bu da uzaydaki varlıkların korunması ile siber savunmayı iç içe bir konu haline getirmektedir.

Tüm bu öngörüler, siber güvenlik ve siber savaş konusunun dinamik ve gelişen bir cephe olduğunu göstermektedir. Devletler ve kurumlar, sadece bugünün tehditlerine karşı değil, ufukta beliren geleceğin karmaşık saldırı senaryolarına karşı da hazırlık yapmak durumundadır. Uluslararası işbirliği, normların belirlenmesi ve yeni teknolojilere yatırım, bu alanda ön plana çıkan gerekliliklerdir.

Sektörel Bazda Siber Savaşların Ekonomik Etkileri

Siber saldırılar her ne kadar dijital ortamda gerçekleşse de, etkileri somut dünyadaki sektörlere yansımakta ve ekonomik zararlara yol açmaktadır. Bu bölümde teknoloji, finans, altyapı ve enerji gibi dört kritik sektör üzerinden siber savaşların ekonomik etkileri örneklerle ele alınacaktır.

Teknoloji Sektörü

Teknoloji sektörü hem siber saldırıların hedefi olması hem de diğer sektörlere yayılan etkileri nedeniyle özel bir öneme sahiptir. Büyük teknoloji şirketleri ve yazılım tedarikçileri, siber casusluk ve tedarik zinciri saldırılarının odağındadır. SolarWinds olayında görüldüğü gibi, bir yazılım üreticisinin sistemine sızılması, onun müşterisi konumundaki binlerce kurumu etkilemiştir. Benzer şekilde 2017'de yaşanan bir başka olay, global ölçekte kullanılan CCleaner adlı popüler bir yazılımın güncelleme sunucusuna sızılmasıydı; bu saldırıda saldırganlar, yazılımın yaygın kullanıcı kitlesini arkadan vurmayı hedeflemişlerdi. Teknoloji devleri de zaman zaman siber saldırılardan ekonomik darbe alabilmektedir: Örneğin 2014'teki Sony Pictures saldırısı, şirketi hem maddi zarara uğratmış (filmler sızdırılmış, sistemler günlerce kapalı kalmış) hem de itibar kaybı yaşatmıştır. Bu gibi olaylar, teknoloji firmalarının hisse değerlerinde düşüşlere, müşterilerin güven kaybetmesine ve ciddi hukuki cezalara yol açabilmektedir. Ayrıca teknoloji sektörüne yönelik siber saldırılar, yenilikçiliği de baltalayabilir. Ar-Ge departmanlarından çalınan tasarımlar veya ürün geliştirme bilgilerinin rakip ülkelere sızması, ilgili şirketin rekabet avantajını yok edebilir. Örneğin Çin kaynaklı hacker gruplarının Amerikan yarı iletken ve telekom firmalarından teknoloji sırları çalması, bu alanda Çin'in ilerlemesini hızlandırırken ABD'li şirketlerin pazar payını ve gelecekteki

gelirlerini riske atmıştır. Bu durum, küresel teknoloji yarışında haksız avantajlar ve ekonomik dengede kaymalar ortaya çıkarabilmektedir. Sonuç olarak, teknoloji sektörü şirketleri siber güvenliğe milyarlarca dolarlık bütçeler ayırmak zorunda kalmakta, bu da tüketicilere ve genel inovasyon ekosistemine maliyet olarak yansımaktadır.

Finans Sektörü

Finans sektörü, siber saldırganların en gözde hedeflerinden biridir; zira doğrudan para ve değerli veriler söz konusudur. Bankalar, borsalar, ödeme sistemleri ve kripto para platformları, her gün sayısız siber saldırı girişimine maruz kalmaktadır. Siber savaş bağlamında özellikle düşman devletler veya örgütler, bir ülkenin finansal istikrarını bozmak için planlı saldırılar yapabilir. Örneğin 2016 yılında Bangladeş Merkez Bankası'nın SWIFT sistemine sızan Kuzey Kore bağlantılı hackerlar, 81 milyon dolarlık hileli para transferi gerçekleştirmişlerdir – ki bu saldırı doğrudan finansal kazanç amaçlı olsa da uluslararası bankacılık sistemine duyulan güvene de darbe vurmuştur. Devlet aktörleri, bazen finansal sistemi kaosa sürüklemek veya ekonomik baskı yaratmak amacıyla siber araçlara başvurabilir. Rusya'nın 2015'te Ukrayna maliye bakanlığını ve ulusal hazinesini hedef alan siber saldırıları, ülkenin finansal işlemlerini aksatmayı hedeflemiştir. Bir diğer endişe verici senaryo, bir ülkenin borsasına veya büyük bankalarına yapılacak koordineli bir saldırıyla, hesapların silinmesi veya işlemlerin manipüle edilmesidir. Böyle bir durumda piyasalarda panik oluşması, hisse değerlerinin çakılması ve yaygın bir ekonomik kriz olasılığı gündeme gelebilir. Finans sektörünün bir diğer zayıf karnı da kişisel verilerin ve kimlik bilgilerinin çalınmasıdır. Büyük ölçekli veri ihlallerinde milyonlarca kullanıcının kredi kartı, banka hesabı ya da kimlik bilgileri çalınabilmekte, bunlar karaborsada satılarak hem bireylere hem finans kuruluşlarına zarar verilmektedir. Örneğin 2017'de ABD'deki Equifax veri ihlalinde 147 milyon kişinin finansal bilgileri sızdırılmıştır. Bu tür olayların ekonomik maliyeti, dolandırıcılık işlemleri, hukuki tazminatlar ve güven kaybıyla ortaya çıkan müşteri kayıplarıyla ölçüldüğünde milyarlarca doları bulmaktadır. Tüm bu riskler nedeniyle finans sektörü, siber güvenlik yatırımlarını en fazla artıran sektörlerden biri olmuştur. Bankalar, güvenlik için her yıl milyarlar harcarken; uluslararası düzenleyici kurumlar da finansal sistemin siber dayanıklılığını artırmak için yeni standartlar getirmektedir. Ancak saldırgan ile savunan arasındaki mücadele durmaksızın devam etmekte, yenilikçi saldırı yöntemleri finans sektörünü tehdit etmeyi sürdürmektedir. Özellikle son dönemde kripto para borsalarına yönelik siber soygunlar (örneğin 2022'de bir kripto platformundan 600 milyon dolar çalınması gibi) yeni cepheler açmıştır. Sonuçta finans sektörü, siber savaşlarda ulusal ekonomileri hedef alan stratejik bir cephe olarak önemini korumaktadır.

Altyapı ve Ulaşım Sektörleri

Kritik altyapılar, bir ülkenin ekonomisinin can damarı konumundadır. Ulaşım ağları (havayolu, demiryolu, karayolu), su temini, atık su arıtma tesisleri, kamu hizmetleri gibi altyapılar, siber saldırıların hedefi olduklarında ekonomide çarpan etkisiyle büyük kayıplara neden olabilirler. Örneğin ulaşım sektörüne bir siber saldırının etkisini ele alalım: Bir havayolu şirketinin veya hava trafik kontrol sisteminin siber saldırı nedeniyle devre dışı kalması, uçuşların iptaline, binlerce yolcunun mağdur olmasına ve ticari faaliyetlerin kesintiye uğramasına yol açar. 2018'de İngiltere'nin Heathrow Havalimanı'nın bilgi sistemlerine yönelik bir siber saldırı girişimi, havalimanı operasyonlarını aksatmış ve maddi kayıplar doğurmuştur. Benzer şekilde, deniz taşımacılığında limanların veya gemi navigasyon sistemlerinin hacklenmesi, küresel ticaret akışını sekteye uğratabilir. 2017'de NotPetya saldırısı sonucu Maersk firmasının liman operasyonlarının durma noktasına gelmesi, dünya ticaretinin ciddi ölçüde aksamasına yol açmıştı. Demiryolu altyapıları da siber savaş senaryolarında kritik hedefler arasındadır. Sinyalizasyon sistemlerinin bozulması tren kazalarına veya sefer iptallerine sebep olabilir. 2016 yılında bir Avrupa ülkesinde (Belçika) demiryolu şirketinin sistemleri fidye yazılımla vurulmuş, tren seferlerinde aksamalar yaşanmıştır. Ulaşım sektöründe meydana gelen her aksama, çalışanların işe gidememesi, ürünlerin zamanında teslim edilememesi gibi ikincil etkilerle ekonomi üzerinde çığ etkisi yaratır. Kentsel altyapılar da dijital tehdit altındadır. Akıllı şehir uygulamalarının artmasıyla, akıllı trafik ışıkları, elektrikli otobüs şarj istasyonları, güvenlik kameraları gibi sistemler de potansiyel saldırı yüzeyi sunmaktadır. Bu sistemlerin çalışmaz hale gelmesi şehir hayatını kaosa sürükleyebilir ve ekonomik faaliyetleri durma noktasına getirebilir. Örneğin bir şehrin trafik yönetim sistemine sızılarak tüm ışıkların kırmızıda kalmasına yol açılması bile ciddi ekonomik kayıp demektir (zaman ve yakıt kaybı, lojistik gecikmeler vb.). Siber savaş durumunda bir ülkenin kritik kamu hizmetleri de hedef alınabilir. Su ve kanalizasyon idarelerinin kontrol sistemlerine yönelik saldırılar, su kesintilerine veya suyun kirlenmesine neden olabilir. 2021'de ABD Florida'da bir su arıtma tesisine sızan saldırganın, içme suyuna aşırı kimyasal karıştırmaya çalışırken son anda fark edilip engellenmesi, bu alandaki riskin altını çizmiştir. Böyle bir saldırının başarılı olması durumunda hem halk sağlığı tehlikeye girecek hem de temiz su temini için büyük masraflar yapılması gerekecektir. Neticede altyapı ve ulaşım sektörleri, siber saldırıların ekonomik ve toplumsal etkilerinin çok yüksek olacağı alanlardır. Buralara yönelik her saldırı, onarım maliyetleri, hizmet kesintileri ve güven kaybı üzerinden ekonomiye darbe vurur. Devletler bu nedenle kritik altyapıların siber güvenliğini milli güvenlik meselesi olarak görüp, operatörlerle sıkı işbirliği içinde koruma çabasındadır.

Enerji Sektörü

Enerji sektörü, hem ekonomik değeri hem de diğer tüm sektörlerin işleyişi için temel olması nedeniyle siber savaşların belki de en stratejik hedefidir. Elektrik şebekeleri, petrol ve doğalgaz boru hatları, nükleer tesisler ve rafineriler gibi enerji altyapıları, bir ülkenin can damarıdır. Bu alanlarda gerçekleşecek bir siber saldırı, ekonomiyi felç edebileceği gibi ulusal güvenliği de doğrudan tehdit eder. Elektrik şebekelerine yönelik siber saldırıların gerçekleştirilmiş örnekleri mevcuttur. Daha önce değindiğimiz Ukrayna'daki elektrik kesintileri, kötü amaçlı yazılımlarla dağıtım merkezlerinin uzaktan kumanda edilmesi sonucu ortaya çıkmıştı. Bu saldırılar, kış ortasında binlerce insanı elektriksiz bırakmış, güvenlik endişelerine yol açmıştı. Benzer bir saldırı çok daha büyük ölçekli bir ülkede gerçekleşse, sadece ekonomik kayıp değil, can kaybı dahil büyük bir insani kriz de söz konusu olabilir. Örneğin ABD'de tüm doğu yakasını hedef alan bir şebeke saldırısının, trilyonlarca dolarlık zararın yanında, hastanelerin çalışamaz hale gelmesiyle can kayıplarına varacak sonuçlar doğurabileceği senaryolarla tartışılmaktadır. Bu nedenle enerji şebekelerinin siber güvenliği üzerinde uluslararası düzeyde çalışmalar yapılmakta, NATO ve AB gibi oluşumlar bu konuda üye ülkelere destek vermektedir. Petrol ve doğalgaz altyapıları, ekonominin diğer kritik unsurlarıdır. Boru hatları, sondaj tesisleri, LNG terminalleri gibi noktalar artık endüstriyel kontrol sistemleriyle (SCADA) işletilmektedir ve bunlar siber saldırıya maruz kalabilir. 2021'de ABD'de Colonial Pipeline şirketine yapılan fidye yazılım saldırısı, doğrudan petrol akışını kesmemiş olsa da şirket tedbir amaçlı boru hattını kapatmak zorunda kalmış ve günlerce yakıt ikmali yapılamaması sonucu bölgede panik alımları ve fiyat artışları yaşanmıştır. Bu olaydan çıkarılan ders, enerji altyapılarının ne denli kırılgan olabileceği ve bir siber saldırının dolaylı bile olsa enerji arzını keserek ekonomik zarara yol açabileceğidir. Bir devlet aktörünün kasıtlı olarak bir ülkenin enerji altyapısını hedef alması ise açık bir savaş ilanı sayılabilecek tehlikeli sonuçlar doğurabilir. Örneğin İran ile ABD arasındaki gerilimde, İranlı hackerların 2012'de Suudi Aramco petrol şirketine "Shamoon" adlı zararlı yazılımla saldırıp 30 bin bilgisayarı silmesi, bölgesel enerji piyasalarını tedirgin etmiş ve Suudi Arabistan'ın petrol üretim operasyonlarını aksatmıştır. Nükleer enerji santralleri de siber savaş bağlamında özel ilgi gerektirir. Stuxnet saldırısı, bir nükleer tesisin siber yöntemlerle fiziksel hasara uğratılmasının mümkün olduğunu ortaya koymuştu. Bir nükleer santralde güvenlik sistemlerinin devre dışı bırakılması ya da reaktörlerin kontrol dışı kalmasına yol açacak bir siber sabotaj, felaketle sonuçlanabilir. Bu nedenle nükleer tesisler, en katı siber güvenlik önlemleriyle korunmaya çalışılmaktadır. Ancak bu tesislerin tedarik zincirindeki yazılımlar veya bakım ekipmanları üzerinden dolaylı saldırılar da ihtimal dahilindedir. Enerji sektörünün önemi ve savunmasızlığı, siber uzaydaki çekişmelerde bu alanı ön plana çıkarmaktadır. Ülkeler arasındaki örtülü çatışmalarda enerji şirketlerine ve altyapılarına sıkça casusluk faaliyetleri yapılmakta; saldırı durumunda nerelerin hedef alınabileceğine dair hazırlıklar yapılmaktadır. Enerji şirketleri de bu yüzden artık sadece endüstri mühendisleri değil, siber güvenlik uzmanlarını da istihdam etmekte; olası saldırıları tespit edip bertaraf etmek için 7/24 izleme merkezleri kurmaktadır. Yine de enerji sektörü, yüksek risk – yüksek ödül dengesi nedeniyle siber saldırganlar için cazip bir hedef olmaya devam etmektedir.

Sonuç

Siber güvenliğin küresel önemi ve siber savaşların etkileri üzerine yaptığımız bu kapsamlı inceleme, 21. yüzyılın dijital dünyasında güvenlik ve istikrarın ne denli kırılgan hale gelebildiğini gözler önüne sermektedir. İnternet ve dijital teknolojiler, insanlığa muazzam kolaylıklar ve ekonomik fırsatlar sunarken, bir yandan da devletlerin ve toplumların karşısına daha önce tecrübe edilmemiş boyutta tehditler çıkarmıştır. Siber uzay, ülkeler arası rekabetin ve çatışmanın yeni cephesi olarak ortaya çıkmıştır. Makalenin başında ele alınan somut olaylar, siber savaşların soyut bir tartışma konusu olmaktan çıkıp gerçek dünyada yıkıcı sonuçlar doğurduğunu kanıtlamıştır. 2007'de Estonya'ya yapılan siber saldırılar, milli ekonomiyi hedef alan dijital taarruzların mümkün ve etkili olduğunu tüm dünyaya göstermiş; NATO gibi güvenlik örgütlerini stratejilerini güncellemeye sevk etmiştir.

Stuxnet, dijital bir silahın fiziksel dünyada çok somut tahribat yaratabileceğini ispatlayarak siber ve fiziksel savaş ayrımını flulaştırmıştır. WannaCry ve NotPetya gibi olaylar, bir siber saldırının kontrolsüz biçimde yayılarak küresel ekonomik zararlara yol açabileceğini ortaya koymuştur. SolarWinds ise en korunaklı sanılan tedarik zincirlerinin bile zayıf halka olabileceğini ve siber casusluğun uluslararası ilişkilerde kriz sebebi sayılabilecek boyuta ulaştığını göstermiştir. Ukrayna-Rusya savaşı ise hibrit savaş konseptinde siber cephenin fiilen nasıl işletildiğine dair derslerle doludur; siber saldırılar fiili çatışmaları tamamlayıcı rol oynamış, bazen de öncü kuvvet olarak kritik sistemleri felç etmiştir. Rusya ve Çin örneklerinde gördüğümüz üzere, büyük güçler siber alana ciddi yatırımlar yapmakta ve bunu siyasi-askeri hedefleri için kullanmaktadır. Rusya'nın siber operasyonları demokratik toplumların iç işlerine karışmaktan komşu ülkelerin altyapılarını sabote etmeye uzanan bir yelpazede gerçekleşirken; Çin daha ziyade uzun vadeli stratejik avantaj peşinde koşarak ekonomik ve teknolojik istihbarat toplamaya odaklanmıştır. Her iki durumda da siber faaliyetler, uluslararası rekabetin ve hatta çatışmanın ayrılmaz bir parçası haline gelmiştir. Bu durum, devletlerin siber caydırıcılık ve savunma politikalarını önceliklendirerek yeni doktrinler geliştirmesine yol açmıştır. ABD'nin yaklaşımı, böylesi tehditlere karşı bir model sunmaktadır: Kurumsal yapılanmalar (CISA gibi) ile ulusal direnci artırmak, askeri kapasite (USCYBERCOM) ile tehdidi kaynağında durdurmak ve uluslararası arenada

normlar ile caydırıcılık tesis etmek. Ancak bu modelin başarısı, saldırıların gerçekleşmemesiyle değil, gerçekleştiğinde etkisinin minimize edilmesiyle ölçülebilmektedir. Zira siber savaş alanında %100 güvenlik imkânsız görünmektedir; önemli olan, risklerin yönetilmesi ve hızlı toparlanma (resilience) kapasitesinin oluşturulmasıdır. Savaşın değişen doğasına baktığımızda, dijitalleşme ve hibrit tehditler çağında yaşadığımız gerçeği netlik kazanmaktadır. Geleceğin muharebelerinde tanklar ve tüfekler kadar, zararlı yazılımlar ve algoritmalar da rol oynayacaktır. Devletler arası güç mücadeleleri, toplumların zihinlerini etkilemeye yönelik dezenformasyon kampanyaları ve kritik altyapılara yönelik siber sabotajlarla iç içe geçecektir. Bu nedenle, 21. yüzyılın güvenlik stratejileri dijital boyutu hesaba katmadan eksik kalacaktır. NATO gibi ittifakların siber savunma planları yapması, ülkelerin siber ordular kurması ve uluslararası hukukun bu alana eğilmeye başlaması, bu değişimin doğal sonucudur. Ekonomi cephesinde ise, siber saldırıların sektörlere göre çok boyutlu etkileri olduğu görülmüştür. Teknoloji şirketleri ve bilişim altyapıları hem hedef hem araç olarak bu resmin merkezindedir; finans sektörü doğrudan ekonomik istikrarla ilgili olduğu için kritik önemdedir; ulaşım ve şehir altyapıları toplum hayatını aksatacak sonuçlar doğurabilir; enerji sektörü ise her şeyin temelinde olması nedeniyle bir nevi "stratejik hedef" konumundadır. Bu sektörlerde alınacak önlemler, yapılacak yatırımlar, geliştirilecek acil durum planları artık ulusal güvenlik planlamasının bir parçası haline gelmiştir. Kritik altyapıların dayanıklılığı, bir ülkenin siber savaş koşullarında ayakta kalabilmesi için belirleyici olacaktır. Sonuç olarak, "siber güvenliğin küresel önemi" ifadesi artık teorik bir vurgudan ziyade pratik bir zorunluluğa işaret etmektedir. Devletler, şirketler ve bireyler, dijital dünyanın sağladığı imkanların yanı sıra getirdiği risklerle de yüzleşmek durumundadır. Siber savaşlar, klasik savaş kavramını dönüştürmüş; coğrafi mesafelerin anlamını yitirdiği, saldırgan ile kurbanın her an rollerinin değişebildiği bir arena yaratmıştır. Bu yeni arenada başarılı olabilmek için uluslararası iş birliği, bilgi paylaşımı ve barış zamanında önleyici tedbirler almak hayati önem taşımaktadır. Aksi takdirde, giderek dijitalleşen küresel ekonomimiz ve güvenlik düzenimiz, tek bir klavye darbesiyle sarsılabilecek bir kırılganlıkta kalacaktır.

Kaynaklar:

- Valeriano, B. & Maness, R. (2015). Cyber War versus Cyber Realities: Cyber Conflict in the International System. Oxford University Press (Estonya 2007 saldırısının ekonomik etkileri)
- Kaspersky. (2022). Ransomware WannaCry: All you need to know. (WannaCry saldırısının küresel maliyeti)
- Wolff, J. (2021). How the NotPetya attack is reshaping cyber insurance. Brookings Institution (NotPetya saldırısının ekonomik zararı)
- Ratnam, G. (2021). Cleaning up SolarWinds hack may cost as much as $100 billion. Roll Call (SolarWinds saldırısının maliyet tahmini)
- Tate, R. (2022). Transparent Cyber Deterrence. Joint Force Quarterly, NDU Press (ABD siber caydırıcılık stratejisi ve maliyet yükleme politikası)
- Booz Allen Hamilton. (2020). Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations. (Rus GRU siber operasyonlarının sonuçları)
- Booz Allen Hamilton. (2022). China's Cyberattack Strategy Explained. (Çin'in siber saldırı stratejileri, savaş eşiği altı yaklaşımı)
- Federal Bureau of Investigation. (2019). China: The Risk to Corporate America (Executive Summary). (Çin kaynaklı fikri mülkiyet hırsızlıklarının ABD ekonomisine maliyeti)
- The Guardian. (2015). OPM hack: 21 million people's personal information stolen, federal agency says. (Çin'e atfedilen OPM saldırısı)
- Sia Partners. (2023). Hybrid Warfare: How Cyber Warfare is Transforming International Relations. (Siber savaşların savaş konseptine etkisi ve örnekler)

Prof.Dr. Murat KOÇ / Çağ Üniversitesi Bölgesel Güvenlik Çalışmaları Uygulama ve Araştırma Merkezi