dipam

DİPLOMATİK İLİŞKİLER ve POLİTİK ARAŞTIRMALAR MERKEZİ
CENTER for DIPLOMATIC AFFAIRS and POLITICAL STUDIES

ANALİZ

ÇİN'İN SİBER GÜVENLİK POLİTİKALARI:
BÜYÜK GÜÇLERİN YENİ REKABET ALANI SİBER UZAY

Larissa KUMAŞ

NİSAN 2024 Sayı: 28

ÇİN'İN SİBER GÜVENLİK POLİTİKALARI: BÜYÜK GÜÇLERİN YENİ REKABET ALANI SİBER UZAY

Günümüzde, siber uzay kavramı, dijitalleşen dünyada giderek artan bir öneme sahiptir. Her geçen gün birbirine daha fazla bağlanan ülkeler ve küresel şirketler, siber uzayda giderek artan bir rekabet ve güvenlik tehdidiyle karşı karşıya kalmaktadırlar. Siber suçlar, sadece bireylerin veya kurumların değil, tüm ulusların güvenliğini tehdit eden ciddi bir sorun haline gelmiştir. Öyle ki, siber saldırıları, askeriyede adeta bir devrim yaratarak yeni bir savaş meydanının doğmasına sebep olmuştur. Bu gerçeklik ülkelerin dış politikalarına yön vererek günümüzde uluslararası ilişkilerin yapıtaşını oluşturmaktadır.

Uluslararası Güvenlikte Siber Uzay

Peki nedir bu ülkelerin dış politikalarında önemli bir araç olan siber uzay? Siber uzay, tanımına göre tüketici bilgisayarları, elektronikler ve iletişim ağlarından oluşan, tüketicinin dünyaya bağlı olduğu yerdir. Siber uzay, fiziksel dünyaya ait olmadığı için fiziksel yasalar siber suçlarına uygulanmaz. Siber suçların yoğun gözlemlendiği ülkelerde, hükümetler tarafından ayrı bir dizi siber yasa çıkarılmış ve bu yasalar, siber kullanıcılarına siber güvenlik sağlamak amacıyla oluşturulmuştur. Bu tür siber yasalar, insanların ahlak veya yasa dışı faaliyetlerini izlemek ve engellemek için gereklidir. Yaygın siber suçlar faaliyetleri arasında bilgisayar korsanlığı (hacking), hırsızlık, kara para aklama, terörizm ve korsanlık yer alır.

Cybersecurity Ventures tarafından yapılan tahminlere göre, siber suçların yıllık maliyetinin 2025 yılına kadar dünya genelinde 10,5 trilyon dolara ulaşması beklenmektedir[1]. Özellikle Amerika Birleşik Devletleri (ABD), uzun yıllardır veri ihlali maliyeti açısından dünya lideri konumunda bulunmaktadır. International Business Machines (IBM) raporlarına göre, 2023 yılında Amerika Birleşik Devletleri'nde bir veri ihlalinin maliyeti 5,09 milyon doları aşmıştır.[2] Bu rakamlar, siber güvenliğin artık sadece bir teknoloji sorunu olmadığını, aynı zamanda ekonomik ve siyasi bir mesele haline geldiğini göstermektedir.

Öte yandan, jeopolitik gerilimlerin artmasıyla birlikte, siber tehditlerin de arttığı gözlemlenmektedir. Özellikle 2022'de başlayan Rusya-Ukrayna savaşı, kuruluşların %97'sinin siber tehditlerde artış yaşamasına neden olmuştur.[3] Özellikle devletler arası ilişkilerde, siber uzayın giderek daha fazla kullanılmasıyla, siber güvenlik konusundaki endişeler de artmaktadır. Bu bağlamda, siber güvenliğin önemini anlamak ve etkili bir şekilde ele almak, uluslararası toplumun en öncelikli görevlerinden biri haline gelmiştir

Devletler özelinde, bu tehditleri ve siber kapasiteyi genişletme amaçlarını üç

[1] Esentire, 2023 Official Cybercrime Report https://www.esentire.com/resources/library/2023-official-cybercrime-report

[2] IBM, Cost of a Data Breach Report 2023. https://www.ibm.com/reports/data-breach

[3] Accenture, State of Cybersecurity Resilience 2023, s. 25 https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf

doğrultuda incelemek mümkündür[4]: Diğer devletlerin kritik altyapılarına sızarak onları güvenlik tehditlerine karşı caydırmak; Siber casusluk yoluyla bilgi edinerek, devletlerin askeri gelişimlerinde daha hızlı ilerlemeleri için bilgi birikimini artırmak; Teknolojik ilerlemenin sağlandığı alanlarda ekonomik kazanımlar elde etmek (örneğin, endüstriyel casusluk yoluyla). Bu anlamda büyük bir siber güç olan Çin'in devlet kabiliyetlerinin analiz edilmesi, diğer devletlere nispetle bu alanda önde olması da göz önünde bulundurulduğunda son derece önemlidir.

Çin'in Siber Güç Olarak Yükselişi ve Merkezi Siber Kontrol Vizyonu

Çin için siber güvenlik, stratejik bir öncelik haline gelmiştir. Ülke, geleneksel bir büyük güç olma hedefiyle birlikte dijital alanda liderlik rolünü üstlenmeyi amaçlamaktadır. Son yıllarda, dijital teknolojilere verilen politik önem, ciddi ölçüde artmıştır. Çin'in siber hedefleri, askeri, ekonomik ve politik alanları kapsamaktadır ve istihbarat toplama, iç gözetim ve genel güvenliği sağlama gibi stratejiler benimsemektedir. Bu adımların temel amacı, parti-devletin gücünü ve meşruiyetini güçlendirmektir.

Çin'in siber güvenlik politikalarının merkezinde, sosyal kredi sistemi gibi öne çıkan inisiyatifler bulunmaktadır. Sosyal kredi sistemi, bireylerin güvenilirliğini kişisel ve davranışsal verilere dayalı olarak değerlendirerek toplum içinde bir güvenlik ve kontrol mekanizması oluşturmayı amaçlamaktadır. Sosyal kredi sisteminin altında büyük siber güvenlik riskleri yatmaktadır: Üçüncü parti hizmetler, Çin teknoloji firmalarıyla iş birliği yoluyla tüketicilerin verilerini ele geçirerek kredi puanlarıyla ilgili faydalar sunarken, büyük miktarda kişisel veri genellikle görünmez bir şirket ağı üzerinden hareket etmektedir[5]. Bu sistem, bireylerin özel yaşamlarına müdahale etmek ve kişisel özgürlükleri kısıtlamanın yani sıra Çin'in kendi vatandaşlarına karşı yürüttüğü bir tür siber savaş olarak da yorumlanabilir.

Nitekim 2017'de kabul edilen Siber Güvenlik Yasası, Çin'in siber güvenlik politikalarını daha da şekillendirmiştir. Bu yasa, parti tarafından belirlenen siber egemenlik vizyonunu yasal bir çerçeveye oturtmuş ve çeşitli veri erişim imkanları sunarak parti-devletin kontrolünü güçlendirmiştir. Askeri-sivil birleşme politikası ve 2017 yasası çerçevesinde, Çinli telekomünikasyon ve teknoloji şirketleri, hükümetle veri paylaşımı ve siber güvenlik teknolojisi konusunda iş birliği yapmak zorunda bırakılmıştır ve Huawei gibi telekomünikasyon şirketleri teşvik edilerek, gelişmekte olan ve bazı gelişmiş ülkelerde bir dizi siber ve veri güvenlik açığı yaratan gelişmeler desteklenmektedir.[6] Çin hükümeti, yine parti içi gözetim ihtiyaçlarından kaynaklanan siber güvenlik ve 5G bağlantısını birbirine entegre etmektedir. 5G, yerel ticaret devleri için gelir yaratırken aynı zamanda Çin Komünist Partisi'nin (ÇKP) yabancı ağlara erişimini de genişletmektedir.

Bu politikaların, liderlik kapasitesine ulaşmak için gerekli olan rejim bütünlüğünü güçlendirmek amacıyla iç

[4] Hjortdal, China's Use of Cyber Warfare: Espionage Meets Strategic Deterrences. s. 3 DOI:10.5038/1944-0472.4.2.1

[5] UC Berkeley (2020). Uncovering the Risk Networks of Third-Party Data Sharing in China's Social Credit System.

[6] Williams, B.K.(2021) "Evaluating China's Road to Cyber Super Power" https://www.osti.gov/servlets/purl/1830481

politikaya yansıdığı ve sonrasında dış politikaya etki ettiği görülmektedir. Çin, siber alanda gücünü artırmak ve uluslararası alanda etkin bir konuma gelmek için siber güvenlik politikalarını aktif bir şekilde uygulamaya devam edeceği anlaşılmaktadır.

Asya Pasifik'te Siber Savaş

ÇKP'nin Ulusal Ekonomik ve Sosyal Kalkınma için 14. Beş Yıllık Planı ve 2035 Uzun Vadeli Hedefleri, açık şekilde bir Siber Süper Güç olma arzusunu belirtmektedir.[7] Bu arzular doğrultusunda siber kapasitesini genişletmeye çalışan Çin'in ABD'ye karşı siber saldırılarını, kritik altyapılarına sızarak güvenlik tehditlerine karşı caydırma; siber casusluk yoluyla, askeri gelişimini daha hızlı ilerletmek için bilgi birikimini artırma ve teknolojik ilerlemenin sağlandığı alanlarda ekonomik kazanımlar elde etme amaçları doğrultusunda gerçekleştirdiğini gözlemlemek mümkündür.

Bu bağlamda, Çin'in ABD'ye karşı geliştirdiği siber silahların da bahsedilen amaçların pratikteki hali olduğu düşünülebilir. Çin'in "önleyici keşif" olarak nitelendirilen siber saldırılarının[8], uzun vadede hedefinin Amerikan ekonomisini ve askeri gücünü aşmak olduğu yorumlanabilir. IP Komisyonu raporuna göre, fikri mülkiyet hırsızlığından kaynaklanan ABD ekonomik yıllık kaybının 300 milyar doların üzerinde olduğu tahmin etmekte ve bu tür hırsızlıkların %50 ila %80'inin Çin tarafından gerçekleştirildiği belirtilmektedir.[9]

Nitekim bu bağlamda gerçekleşen ve endüstriyel casuslukta bir dönüm noktası olarak kabul edilen Operasyon Aurora, 2010 yılında ABD özel sektör şirketlerini hedef alan Çin kaynaklı bir dizi siber saldırıdır. Tehdit aktörleri, Yahoo, Adobe, Dow Chemical, Morgan Stanley, Google ve daha birçok şirketin ağını tehlikeye sokan bir e-dolandırıcılık (phishing) kampanyası yürüterek ticari sırlarını çalmak için bu şirketleri hedef almıştır. Google, kurban olduğunu doğrulayan ve belirli Çinli insan hakları aktivistlerinin Gmail hesaplarının tehlikeye girdiğini kamuoyuna açıklayan tek şirket olmakla beraber olayı Çin'e atfetmiştir.

Operasyon Aurora'nın ardından 2016'da dönemin ABD Başkanı Barack Obama ve Çin Devlet Başkanı Xi Jinping'in fikri mülkiyet hırsızlığını önlemeyi amaçlayan geniş çaplı bir siber casuslukla mücadele anlaşmasından dokuz ay sonra, Çin'in Silikon Vadisi şirketleri, askeri şirketler ve diğer ticari hedeflere neredeyse günlük düzeyde gerçekleştirdiği siber saldırılarda büyük bir düşüş olduğu belirtilmiştir.[10] Ancak, Başkan Donald J. Trump'ın yönetiminin başlaması ve Çin ile ticaret savaşlarının ve diğer gerilimlerin

[7] Xinhua News Agency (2021) "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035," https://cset.georgetown.edu/publication/china-14th-five-year-plan/
(Xinhua Çinin devlet tarafından yönetilen resmi medya kuruluşudur. Yazı, Georgetown Üniversitesi tarafından İngilizce'ye çevrilmiştir)

[8] Rugina, J.M. 2023, Economic Cyber Espionage: The US-China Dilemma. https://doi.org/10.5152/JIRS.2023.23014

[9] The Commission on the Theft of American Intellectual Property Report (2013) https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report.pdf

[10] FireEye Report, (2021), Red Line Drawn: China recalculates its use of cyber espionage. https://www.mandiant.com/sites/default/files/2021-09/rpt-china-espionage-1.pdf

tırmanmasıyla birlikte, bilgisayar korsanlığı faaliyetleri yeniden başlamıştır.[11] Trump'ın gümrük vergilerindeki artışı desteklediği 'Amerika'yı Yeniden Harika Yap' politikaları ile ABD'li işletmelerin çıkarlarına yönelik küresel teknolojik lider olma çabasının, diplomatik gerilimlerle birleştiğinde siber güvenlik konusunda büyük bir tehdit oluşturduğu görülmüştür.

Siber güvenlikteki tehditler, teknoloji ve büyük veri sektörlerindeki ticaret savaşını daha da artırmaktadır. Ticaret ve siber güvenlik arasındaki bu döngüsel tehdit yapısı, 21. yüzyıl ABD-Çin rekabetine yeni bir boyut kazandırmıştır ve yoğunlaşarak artmaya devam etmektedir. Kısa vadede Çin'in, dünyanın önde gelen siber güvenlik ulus devleti olan ABD'yi geride bırakması zor gibi görünmektedir. Çin, ABD'nin verilerini dışarı aktarmak için hedef almaya devam edebilir ve kriz durumunda askeri üstünlük elde etmek için yabancı devletlerin ağlarını haritalayabilir. Siber casusluktan ekonomik veya diplomatik kazanç elde etmek, ÇKP için cazip olabilir ve siber casusluk kampanyaları hızlanabilir.

Bu risklere karşılık olarak Biden yönetimi hem devletler hem de bireyler bazında bazı adımlar atmaktadır. Bireysel seviyede, son yıllarda defalarca gündeme gelen ancak bir eylem alınmayan TikTok uygulamasının ABD'de yasaklanması örnek olarak verilebilir. ByteDance isimli Çin merkezli bir firmanın %60'ına sahip olduğu TikTok'un, ABD hükümet yetkililerinin telefonlarına indirilmesi yasakken yukarıda belirtildiği gibi Çin hükümetinin teknoloji şirketlerini veri paylaşımı konusunda iş birliğini zorunlu kılması endişeleriyle birlikte, ülke genelinde yasaklanması için yasa, ABD Senato'suna sunulmuştur. Benzer şekilde, Avrupa Komisyonu çalışanlarına uygulamayı yasaklayan karar, siber güvenlik tehditlerine dayanarak alınmıştır.

Devletler seviyesinde ise Hint-Pasifik bölgesinde siber güvenlik iş birliğini geliştirmek için Japonya ve Güney Kore ile yapılan son taahhütler gibi bazı gelişmeler bulunmaktadır.[12] Bu taahhütlerde ortaklar, kritik altyapı tehditleri ile ilgili siber tehdit istihbaratını paylaşmanın önemini kabul edilmektedir ve bu iş birliğinin temel amacı, bölgede siber güvenliği artırmaktır.

Tüm bu gelişmeler, ABD-Çin çatışmasında yeni bir evreye geçildiğinin işaretlerini vermektedir; ticaret ve teknoloji savaşları, bugün siber savaşla pekiştirilmiş durumdadır. Bu çatışmaların soğuk savaş izlerini taşıdığı hissedilmektedir, dijital çatışmalarla birlikte istihbarat toplama faaliyetleri ve sabotaj tehdidinin artmasıyla karakterize edilen bir tür savaş olduğu belirtilmektedir. Siber savaşın riskleri bu iki ülkeyi sıcak bir savaşa tekrardan yaklaştırabilir mi sorusu akılları kurcalamaktadır. Net olan bir tek şey vardır ki, ABD-Çin siber savaşının artan tehdidi önünde ciddi tehlikeler bulunmaktadır.

[11] Rugina, J.M. (2023), Economic Cyber Espionage: The US-China Dilemma; Larres, K. (2020). Trump's trade wars: America, China, Europe, and global disorder.

[12] Atlantic Council, Şubat 2024. "To combat Chinese cyber threats, the US must spearhead a

YAZAR HAKKINDA

Larissa Kumaş, Koç Üniversitesi'nde Uluslararası İlişkiler bölümünde lisans derecesini tamamlamış ve İşletme bölümünden çift ana dal lisansını almıştır. DİPAM'da teknolojik gelişmelerin uluslararası ilişkilere etkisini inceleyen Kumaş, siber güvenlik, uzay ve yapay zeka konularında analizler yazmaktadır. Yüksek lisansını siber güvenlik yönetimi üzerine yapmayı planlamaktadır.