Teknoloji Rekabetinde Huawei Bir Tehdit Mi?

Barış ESEN[1]

Makale Gönderim Tarihi: 27 Nisan 2021
Makale Kabul Tarihi: 15 Eylül 2021

Öz

Ticaret savaşı gündeminin yanında teknoloji rekabeti konusunda da Çin, ABD'nin hedefi konumundadır. Hatta ABD ile Çin arasındaki mücadele teknolojik soğuk savaş şeklinde de yorumlanmaktadır. Bu çalışma Huawei'nin ABD için bir tehdit olup olmadığını incelemektedir. ABD yönetimi, dünyada Çin ürünlerinin Amerikan ürünlerinden daha fazla tercih edilmesinden dolayı rahatsız olmaktadır. ABD'yi rahatsız eden noktalardan biri de Amerikalı şirketlerin fikri mülkiyetlerinin Çin tarafından çalındığı şeklindeki iddialardır. ABD, Huawei'yi ulusal güvenliği için tehdit olarak kabul etmektedir. ABD, başta Avrupalı müttefikleri olmak üzere diğer ülkeleri Çinli Huawei ile çalışmaması konusunda uyarmaktadır. Buna karşın Avrupalı ülkelerin çoğu ABD'nin tüm baskılarına rağmen Huawei ile çalışmaya devam etmektedirler.

Anahtar Kelimeler: Ekonomik rekabet, Fikri mülkiyet, Ulusal güvenlik, Uluslararası ekonomi

JEL Sınıflandırması: F50, F51, F52

[1] Doktor Öğretim Üyesi, Beykent Üniversitesi Siyaset Bilimi ve Kamu Yönetimi Bölümü, e-posta: barisesen@beykent.edu.tr, ORCID: 0000-0001-8648-9430, Telefon: 0533 474 06 77.

Does Huawei Pose a Threat to Technology Competition

Abstract

In addition to the trade war agenda, China is the target of the USA in terms of technology competition. Even the struggle between the USA and China is interpreted as a technological cold war. This study examines whether Huawei is a threat to the US. The US administration is uneasy because Chinese products are preferred over US products. One of the points that bothers the USA is the claim that the intellectual property of American companies has been stolen by China. The USA considers Huawei as a threat to its national security. The US warns countries, especially her European allies, not to work with Chinese Huawei. On the other hand, most of the European countries continue to work with Huawei despite all the pressures of the USA.

Keywords: Economic competition, Intellectual property, National security, International economics

JEL Classification: F50, F51, F52

1. Giriş

ABD ile Çin arasındaki ticaret savaşları, Ocak 2017'de Donald Trump'ın Amerika Birleşik Devletleri (ABD) Başkanlığı görevini devralmasıyla başlamış ve 2018-2019 döneminin neredeyse tamamı boyunca gündemde yer almıştır. Ticaret savaşlarının sonuçları ise bu iki ülke ile sınırlı kalmamıştır. Ticaret savaşları, ABD'nin komşuları ile Avrupa ve Çin'in tedarik zinciri ile bağlı olduğu diğer Asya ülkelerine kadar birçok ülkeyi ekonomik açıdan etkilemiştir. ABD'nin yeni gümrük tarifeleri ile başlayan ve sıkı teknoloji kontrolleri ile devam eden süreç sonrası ABD ile Çin arasında ekonomik bir demir perde oluşmuştur (Kennedy, 2019). Bu süreç ile birlikte Çin'in dünyanın geleneksel teknoloji tedarikçileri ile olan ilişkisi değişmiştir. Ticaret savaşları sonrası Çin'in diğer ülkeler ile olan teknoloji işbirliğinde azalmalar söz konusu olmuştur. Çin yönetiminin, ülkenin kendi ekonomik gelişiminde yabancı teknolojiye olan bağımlılığını azaltması gerektiği şeklindeki düşüncesi güç kazanmıştır. Ekonomik açıdan ABD ve Çin için bazı olumsuz sonuçlara neden olan ticaret savaşları, 2020 yılı başında iki ülke arasında imzalanan birinci faz anlaşma ile bir ateşkes sürecine girmiştir.

Ticaret savaşı gündeminin yanı sıra onun bir alt başlığı olarak değerlendirilen teknoloji yarışı konusunda da Çin, ABD'nin hedefi konumundadır.

Çin'in teknoloji ağırlıklı hızlı ekonomik yükselişi ve dünyanın ikinci büyük ekonomisi haline gelmesi ABD'nin küresel ekonomideki hakim konumunu tehdit etmektedir. ABD'yi rahatsız eden noktalardan biri de Amerikalı şirketlerin fikri mülkiyetlerinin Çin tarafından çalındığı şeklindeki iddialardır. ABD, Çin'in fikri mülkiyet hakları hırsızlığı ve siber casusluk ile elde edilen ticari sırlar ile oluşan ekonomik başarı sayesinde kendisine rakip olduğunu öne sürmektedir.

ABD, Çin'in hızlı ekonomik büyümesi ile küresel manadaki hakimiyetinin tehdit altında olduğunu değerlendirmektedir. Dolayısıyla ABD tarafının Çin ile ilgili endişesi salt ekonomik değil, siyasi unsurları da içermektedir. ABD, geçmişte Japonya ekonomisinin 1980'lerdeki yükselişi ve ABD'li şirketleri satın alma yoluyla ele geçirmesinden de rahatsız olmuştur (Nolan, 2012). Japon şirketleri, o dönemlerde Çinli şirketlere benzer şekilde ABD'nin engelleri ile karşılaşmıştır. Dönemin ABD Başkanı Ronald Reagan, 1988 yılında Amerikalı yarı iletken şirketi Fairchild Semiconductor'ın Japon Fujitsu tarafından satın alınmasına engel olmuştur (Wang ve He, 2019). Günümüzde de başta Hauwei olmak üzere Çinli şirketlerin ABD'deki satın alma girişimleri siyasi engeller ile karşılaşmaktadır.

Çin'in dünyada siyasi etkileri de olabilecek hızlı ekonomik büyümesinin barışçıl olmayacağına dair görüşler mevcuttur (Mearsheimer ve Brzezinski, 2005). ABD-Çin arasındaki sorunların, ekonomik ve diplomatik alandan sıcak çatışmaya uzanma riski zaman zaman gündeme gelmektedir. ABD, Çin'i ekonomik gücünü kullanan, ülkelere baskı yapan ve kendi otoriter rejimini yaymaya çalışan revizyonist bir ülke olarak tanımlamaktadır (Department of Defence, 2018). Güney Çin Denizi ve Tayvan gibi gerilim başlıkları olsa da iki ülke arasındaki çatışma, fiziki karşılaşma yerine şimdilik siber ağlar üzerinden yürütülmektedir.

ABD, Çin'in siber saldırılarının, ülkesinin ulusal güvenliğini etkileyebilecek ve dolaylı olarak savunma sektörüne de uzanabilecek hedefli operasyonlar olduğunu iddia etmektedir. ABD'nin küresel bir askeri güç olmasının omurgasında savunma bütçesi ile birlikte teknolojik üstünlüğü yer almaktadır. Teknoloji ile bilgi ve veriye ulaşma imkanı ülkelerin karar alma süreçlerine hız kazandırırken rakiplerinin sürprizlerine karşı hazırlıklı olma imkanı sağlamaktadır (Riikonen, 2019). Devletler, adeta suç organizasyonları gibi, siyasal ya da ekonomik çıkar sağlamak ve bilgiye ulaşmak adına siber korsanlık işlemlerine girişebilmektedir (Demchak, 2016). Çin'in siber yollar ile ABD'deki uzay, altyapı, enerji, nükleer güç, teknoloji, temiz enerji, biyoteknoloji ve sağlık endüstrilerini hedef aldığı değerlendirilmektedir (Iasiello,

2016). ABD ile Çin arasındaki bu mücadele telekomünikasyon sektöründe yoğunlaşan bir siber savaş ya da teknolojik soğuk savaş şeklinde yorumlanabilmektedir.

Bu çalışmanın amacı ABD ile Çin arasındaki Huawei anlaşmazlığının nedenlerini incelemektir. Teknoloji rekabetinde Huawei'nin başta ABD olmak üzere diğer ülkelere bir tehdit olup olmadığı konusundaki soruya yanıt aranmaktadır. Makalede Huawei'nin iki ülke arasında ticaret ve teknoloji savaşlarının bir unsuru olup olmadığı irdelenmektedir. Çalışmada, Çin'in ekonomik yükselişinin arkasındaki itici güçlerden biri olan teknoloji hamlesi ve Çin Malı 2025 gibi hedefler ele alınmaktadır. ABD'nin Huawei'ye dönük güvenlik kaygıları ile birlikte şirketin teknolojik gelişimi anlatılmaktadır. Çalışmada ayrıca 5G teknolojisi konusundaki küresel rekabette Huawei'nin rolüne dikkat çekilmesi hedeflenmektedir. Siber güvenlik kavramına da değinilen çalışmada ABD'nin Huawei'ye karşı aldığı önlemler ve bu önlemlerin şirkete etkisi değerlendirilmektedir. Makale, ABD'nin iddiaları ve şirkete karşı aldığı önlemler ile birlikte Huawei'nin yanıtlarını ortaya koyarak objektif bir sonuca varmayı amaçlamaktadır.

2. Çin'in Teknolojik Hamlesi

Çin, olumlu sonuçlarını son yıllarda görmeye başlasa da ülkenin teknoloji hamlesi çok daha öncelere uzanmaktadır. Çin, 1980'lerden itibaren devlet şirketlerini reforma tabi tutarak onları küresel rekabete hazır devler haline getirmeyi amaçlamaktadır. Pekin yönetimi, teknoloji alanında telekomünikasyon sektörüne ise stratejik bir önem atfetmektedir. Çin, ülke güvenliği için önemli olarak gördüğü telekomünikasyon sektörüne 1980'li yılların başından itibaren yoğunlaşmıştır. Pekin yönetimi, ülkede teknolojiye dayalı sanayinin gelişmesi için anahtar rol oynamıştır ve öncelikle ülkeye yabancı teknolojilerin ithal edilmesi yolunu tercih etmiştir. Bir sonraki aşamada ise yabancı şirketler ile Çinli devlet destekli şirketlerin iş ortaklığı yapmasının önü açılmıştır. Başta Belçikalı, Fransız ve Alman teknoloji şirketleri, Çinli telekomünikasyon şirketleri ile ortaklığa giderken bu yolla yabancı teknolojilerin ülkeye transfer edilmesi sağlanmıştır. Bu yabancı şirketler Çin gibi büyük bir pazara girebilmek için teknoloji transferi konusunda tavizler vermişlerdir (Harwit, 2007).

Çin'in ekonomik yükselişinde yabancı teknoloji şirketlerinin ülkede açtığı araştırma geliştirme merkezlerinin de payı olmuştur. Microsoft'un Asya Araştırma Merkezi'nde yetişen yaklaşık beş bin Çinli yapay zeka uzmanı daha sonra Baidu, Alibaba, Tencent ve Huawei gibi Çinli şirketlerde yönetici olarak çalışmaya başlamışlardır (Lee, 2018). Çin, ayrıca yurtdışına giden

öğrencilerin ülkeye yeniden dönmesini sağlayacak programlar geliştirmiştir. Yetenekli yabancı mühendis, biliminsanı ve araştırmacıların Çin'e gelişine imkan sağlayacak açılımlar yapılmıştır. Dolayısıyla Çin teknolojik gelişmeye sadece maddi açıdan değil insan kaynağı açısından da yatırım yapma yolunu seçmiştir.

Çin Devlet Konseyi tarafından 2010 yılında açıklanan yedi stratejik sektör, teknoloji yoğunluklu alanlar olarak öne çıkmaktadır. Bu yedi sektör sırasıyla; enerji tasarrufu ve çevre koruma teknolojileri, yeni nesil bilişim teknolojileri, biyoteknoloji, yüksek teknolojili ekipman üretimi, yeni enerji, yeni malzemeler ve yeni enerjili araçlar olarak ifade edilmektedir (Holz, 2018). Bu sektörlere devlet dışı aktörlerin yatırımları da teşvik edilirken sektörlerin gayri safi yurtiçi hasıla içindeki payının 2020 yılında % 15'e çıkarılması hedeflenmiştir. Çin'in dünyanın en yenilikçi ülkesi olma hedefi 2049 yılında bilim ve teknolojide dünya lideri olma amacını da taşımaktadır (Kennedy, 2019). Bu amaçla Çin, araştırma ve geliştirme bütçesinin payını giderek artırmaktadır. Çin, 2017 yılı rakamlarına göre 496 milyar dolar ar-ge harcaması ile dünyada bu alanda ikinci ülke konumundadır. ABD ise Çin'in hemen önünde 543 milyar dolar ile ar-ge harcamasında dünya lideri olarak kabul edilmektedir. Gayrisafi yurtiçi hasılaya (GSYH) oran ile bakıldığında ise ABD, GSYH'sinin % 2,7'sini ar-ge harcamasına ayırırken Çin'de ise bu oran % 2,1 civarında seyretmektedir (UIS, 2019). Çin, 2017 yılında Devlet Konseyi'nin aldığı karar çerçevesinde ülkeyi 2030 yılında dünyanın yapay zeka merkezi yapma hedefindedir (Kennedy, 2019).

2.1. Çin Malı 2025

Çin, yabancı şirketlere ve teknolojilere bağımlılığı azaltmayı hedefleyen Çin Malı 2025 isimli ulusal stratejisi ile ileri teknolojide yurt içi üretimini 2025 yılına kadar %70 oranında artırmayı planlamaktadır. Bu strateji ile teknolojide kendi kendine yeten bir ülke olma hedefi ile yabancı teknolojinin Çin'de üretilen teknoloji ile kademeli olarak yer değiştirmesi amaçlanmaktadır. Çin, yüksek teknolojiye dayalı alanlarda yerli şirketlere yüksek oranda sübvansiyon ve ucuz krediler ile destekler sunmaktadır. Çin yönetimi, bu yolla yabancı şirketlere ve teknolojilere bağımlılığı azaltarak yerli şirketlerin Çin pazarındaki ağırlığını artırmayı amaçlamaktadır (Akkemik ve Tuncer, 2019). Bu nedenle Çin Malı 2025, geleneksel olarak yüksek teknoloji üreticisi ülkeler olan Almanya, Japonya, Güney Kore ve ABD'ye bir meydan okuma olarak algılanmaktadır.

Mayıs 2015'te duyurulan Çin Malı 2025 planı, Almanya'nın 2012 yılında açıkladığı Almanya "Endüstri 4.0" programının Çin versiyonu olarak

yorumlanmaktadır. Çin Malı 2025 ile bilgi teknolojileri, robot teknolojisi, uzay ekipmanları, okyanus mühendisliği ekipmanları ve yüksek teknoloji gemiler, demiryolları, enerji tasarrufu ve yeni enerji araçları, güç ekipmanları, yeni malzemeler, ilaç ve medikal araçlar ile tarım makinaları gibi 10 farklı alana öncelik verilmektedir (Holz, 2018). Bu program robotlar, akıllı alıcılar, kablosuz alıcı ağları ve çipler gibi akıllı imalat ürünleri üretimi ile sanayinin modernizasyonunu amaçlamaktadır (Wübbeke vd., 2016). Çin, bu plan ile imalat teknolojilerinde gelişmiş ülkelere yetişmeyi planlamakta, önümüzdeki on yıllarda imalatta süper güç olmayı hedeflemektedir. Plan ile öncü Çinli şirketlerin dünyada rekabet gücüne sahip teknoloji devleri arasına girebileceği tahmin edilmektedir. Çin'de tüketici elektroniği gibi sektörler teknoloji kullanımı açısından yabancı rakipleri ile benzer düzeyde değerlendirilmektedir. Otomotiv ve çelik endüstrisindeki şirketlerin ise teknoloji kullanımında yabancı rakiplerinden daha geri bir konumda oldukları varsayılmaktadır (Wübbeke vd., 2016). Çin yönetimi geride kalan bu şirketlerin uluslararası piyasada daha fazla var olmaları için finansal destekler sunmaktadır.

Çin Malı 2025 planı başarılı olursa, Çinli şirketlerin yerli teknoloji tedarikçileri yardımıyla gelişmiş ülkeler ile aralarındaki teknoloji açığını kapatmalarının mümkün olabileceği tahmin edilmektedir. Bu plan ile Çinli şirketlerin yabancı teknolojilere olan bağımlılığının azaltılması hedeflenmektedir. Çin'in bu stratejisine yönelik dış rahatsızlığın kaynağı, önemli sanayilerde ve teknolojide ülkenin % 70 oranındaki kendine yeterlilik hedefi olarak ifade edilmektedir. İthal ikamesini amaçlayan bu politikalara Dünya Ticaret Örgütü (DTÖ) kurallarını ihlal ettiği iddiası ile Almanya ve ABD karşı çıkmaktadır (Akkemik ve Tuncer, 2019). Çin Malı 2025 ile birlikte ABD'nin küresel ekonomik hakimiyeti de tehdit altına girmektedir. ABD yönetimi Batı'da Çin ürünlerinin Amerikan ürünlerinden daha çok tercih edilmesinden dolayı rahatsızlık duymaktadır. ABD'nin engelleme politikalarından da anlaşılabileceği üzere bu rahatsızlığın odak noktalarından birinin 170'ten fazla ülkede ürün ve hizmet sunan Huawei olduğu düşünülmektedir.

3. Küresel Bir Teknoloji Şirketi Olarak Huawei

Çin'in Silikon Vadisi olarak bilinen Şenzen kentinde 21 bin yuan sermaye ile eski bir subay olan Ren Zhengfei tarafından kurulan Huawei, dünyanın en büyük telekomünikasyon ürünleri ve hizmeti sağlayıcısıdır. 1987 yılında kurulan Huawei, İngiltere merkezli marka değerleme ve strateji danışmanlığı şirketi olan Brand Finance tarafından 2020 yılında dünyanın en değerli 10 markasından biri olarak seçilmiştir (Brand Finance, 2020). Huawei, 65 milyar dolarlık marka değeri ile dünyanın en büyük ikinci akıllı telefon üreticisi

konumundadır. Huawei, sadece telekomünikasyon sektörü ve akıllı telefon pazarında değil bilgisayarlar, akıllı ekranlar, giyilebilir cihazlar, bulut teknolojisi, ağ işlevleri ve nesnelerin interneti konularında da faaliyet göstermektedir. Huawei, bulut hizmetleri, akıllı telefonlar, bilgisayarlar ve ağ sistemlerini birleştirerek entegre çözümler sunmaktadır. Huawei, telekom operatörleriyle birlikte dünya nüfusunun 3'te 1'inden fazlasını birbirine bağlamaya yardımcı olan 1500'ün üzerinde ağa sahiptir (Alkhawajah, 2019). Yaklaşık 194 bin kişinin istihdam edildiği Huawei'nin dünya çapında 21 araştırma ve geliştirme merkezi bulunmaktadır.

3.1. 5G Teknolojisi, Çin ve Huawei

Çin, ağlar üzerinden transfer edilecek bilgilere dair önem arzeden 5G teknolojisine dünyada en fazla yatırım yapan ülke konumunda bulunmaktadır. Çin, aynı zamanda 1 milyarı aşan mobil kullanıcı sayısı ile dünyada bu konuda en büyük pazara sahip ülke konumundadır. Çin, bu yeni nesil teknolojiyi geleneksel şirketlerinin dijital ekonomiye geçişinde bir fırsat olarak değerlendirmektedir. Çin, 5G ile akıllı şehirler, sürücüsüz araçlar ve fabrika otomasyonları gibi alanlarda küresel çapta dijital ekonominin hem altyapısını kurmak hem de yönetmek istemektedir. Yapay zeka ve ağ teknolojilerinin desteklediği bu sistemde Baidu şirketi sürücüsüz otomobiller, Alibaba şirketi akıllı şehirler, Tencent şirketi ise sağlık teknolojileri konularına yoğunlaşmıştır (Kennedy, 2019). Çin, 2013'te Sanayi ve Bilgi Teknolojileri Bakanlığı, Ulusal Kalkınma ve Reform Komisyonu ve Bilim Teknoloji Bakanlığı'nın da içerisinde olduğu 5G Teşvik Grubu adı altında bir yapılanmaya gitmiştir. Bu yapılanma içerisinde üniversitelerin araştırma ve geliştirme bölümlerinin yanı sıra China Mobile, China Telecom ve China Unicom ile Huawei, ZTE, Lenovo, Xiaomi, Oppo ve Vivo gibi teknoloji şirketleri de yer almaktadır (Triolo, 2020).

Çinli teknoloji şirketleri Huawei ve ZTE, 5G altyapıları ile dünyaya yayılmış durumdadırlar. Avrupa, Ortadoğu ve Güneydoğu Asya'da çok sayıda ülke Huawei ile çalışma kararı almaktadır. Huawei, dünyada ondan fazla ülkede 5G kurulumuna yardım etmektedir. Çin, ayrıca Kuşak ve Yol Projesi ile mallarının Avrupa'ya ihracatında yeni koridorlar hedeflemektedir. Çin, bu projede yer alacak katılımcı ülkeler ile lojistik, üretim, ekonomi ve ticaret bağları kurarken üyelere teknoloji ve finansman desteği de sağlamaktadır (Tutan, 2019-2020). Çin, Kuşak ve Yol Projesi üzerindeki ülkelerin 5G altyapısını Huawei ile birlikte gerçekleştirmektedir. Dijital İpek Yolu tanımlamaları yapılırken bilgi teknolojisi altyapı projeleri Çin için bir dış politika aracı olarak kullanılmaktadır (Riikonen, 2019).

Huawei, modern zamanların etki ajanı olarak tanımlanmakta, 17.yüzyıl ile 19.yüzyıl arasında koloni faaliyetleri yürüten Hollanda Doğu Hindistan ve İngiltere Doğu Hindistan Kumpanyası şirketlerine benzetilmektedir (Mills, 2013-2014). Bu iki şirket Avrupa sinai büyümesinde büyük roller üstlenmiştir. Hatta Hollanda Doğu Hindistan Kumpanyası, kendi ordusu ile savaş açıp yabancı toprakları sömürgeleştirecek güce kadar ulaşmıştır. (Acemoğlu ve Robinson, 2019:245) Bahsedilen koloni faaliyetlerini yürüten şirketler devletlerin etki alanlarını ülke dışına taşıyan yapılar olarak kabul edilmektedir. Huawei de benzer şekilde örneğin Afrika kıtasında Çin devletinin etkisinin genişlemesine yardımcı olmaktadır. Çin, Afrika'nın en büyük ticaret ortağıdır ve bu bölgeden hammadde ithal etmektedir. Çin, aynı zamanda Afrika'nın altyapı tesislerini inşa ederken bölgenin lider telekomünikasyon ekipmanı tedarikçisi haline gelmiştir. Huawei, Nijerya ve Kenya'da telekom ve internet altyapı hizmetleri ile bu ülkelerdeki siyasi yapılara Pekin yönetimi adına ulaşma imkanı sağlamaktadır. Çin'in devlet ortaklı girişimi Nijerya devleti için telekomünikasyon uyduları inşa etmiştir. Çin, 500 milyon dolara mal olan bu iş karşılığında Nijerya İletişim Uydu şirketinden pay almıştır (Riikonen, 2019).

5G teknolojisi ile dünyada lider konumda olan Huawei, ülkesinde Çin 2030'da devreye girmesi beklenen 6G konusunda çalışmalara başlamış durumdadır. Çin'in önümüzdeki 5-7 yıl içerisinde baz istasyonları, fiber kablolar, veri merkezleri, antenler ve yazılımlar için yaklaşık 200 milyar dolarlık yatırım yapacağı tahmin edilmektedir (Triolo, 2020). Çinli diğer teknoloji devleri Baidu, Alibaba, Tencent gibi şirketler de 5G yatırımı yapan telekomünikasyon şirketlerinden pay alarak onlara destek olmaktadırlar.

3.2. 5G ve Huawei'ye Dönük Güvenlik Kaygıları

ABD, Huawei'yi entegre telekomünikasyon sistemlerinin güvenliği için tehdit olarak görmektedir. ABD'nin bu kaygısının ardında yatan, Çinli şirketleri bilgi paylaşımı ile yükümlü kılan Çin İstihbarat Kanunu'ndaki 7.maddedir. Çin'in İstihbarat Kanunu'ndaki 24.madde de, istihbarat soruşturmalarında kişilerin ve kurumların bilgi ve belge taleplerini reddedemeyeceği yer almaktadır (Hoffman ve Kania, 2018). Başta 5G olmak üzere telekomünikasyon altyapısına dair ulusal güvenlik endişesi ve vurgusu aslında ABD ile sınırlı değildir. Bu konudaki hassasiyet bizzat Hauwei'nin kurucusu Ren Zhengfei'nin 1994'te Çin Komünist Partisi Genel Sekreteri Jiang Zemin ile görüşmesinde dile getirilmiştir. Huawei kurucusu Ren, Jiang Zemin ile görüşmesinde telekomünikasyon ekipmanlarının ulusal güvenlik meselesi olduğunu belirterek kendi telekom altyapısına sahip olmayan ülkeleri ordusu olmayan devletlere benzetmektedir (Harwit, 2007).

ABD'deki güvenlik kaygısı, telekomünikasyon altyapı sistemlerinin içine yerleştirilebilen arkapı uygulamaları ile hassas verilerin başkaları tarafından elde edilme riski olarak öne çıkmaktadır. Ekonomik istihbarat yoluyla ele geçirilen bilgiler, hem imalat sanayi hem de savunma sanayi için ülkelere belirli avantajlar sağlayabilmektedir. Teknoloji şirketlerine ait bilgiler konusundaki hassasiyet öyle bir noktaya ulaşmıştır ki ABD, bu alanlarda çalışan Çinli öğrencilerin vize sürelerinde kısaltmalara dahi gitmektedir (Kennedy, 2019). Yurtdışındaki Çinli şirketler tarafından elde edilen verilerin daha sonra Çin devleti ile paylaşılabileceğine dair güvenlik kaygıları söz konusu olmaktadır. Nitekim İngiliz Vodafone şirketi 2011 ve 2012'de İtalya'da kullandığı Huawei ekipmanlarında gizli bir arkapı keşfettiğini açıklamıştır (Lepido, 2019). 2003 yılında Amerikalı Cisco, kaynak kodlarını yasadışı yolla kopyalamak ve patentlerini ihlal etmek suçlaması ile Huawei'yi dava etmiştir. Huawei yetkilileri davada kopyalamayı doğrulamış ancak bunun söz konusu yazılım kodları içerisinde yalnızca % 2'lik bir orana denk geldiğini savunmuştur. (Thurm, 2003) Cisco'nun ABD'de Huawei'ye dönük fikri mülkiyet hakları ihlali iddiasıyla açtığı dava başarısızlıkla sonuçlanmıştır. Hatta Cisco CEO'su John Chambers, daha sonra Huawei'nin mükemmel bir şirket ve iyi bir rakip olduğunu söylemiştir (Nolan, 2012). 2010 yılında Motorola, Huaewei'yi eski çalışanları ile işbirliği yaparak ticari sırlarını çalmak ile suçlamıştır. 2017 yılında ise Huawei, ABD'de T-Mobile şirketinin robot teknolojisini çalmaktan suçlu bulunmuştur (U.S. District Court, 2017). 2019 yılında ise Polonya'daki bir Huawei çalışanı Çin hükümeti adına ajanlık yapmaktan tutuklanmıştır. Şirket casusluk suçlamalarını reddederek tutuklanan çalışan ile iş ilişkisini sonlandırdığını duyurmuştur (Gao vd., 2020).

ABD, tüm ülkelere ve özellikle müttefiklerine 5G için Çinli Huawei ile çalışmamaları konusunda uyarı ve çağrılarda bulunmaktadır. Bu uyarı ve baskılar sonrasında, ABD'nin müttefiki olan ülkeler Japonya, Avustralya, Yeni Zelanda ve Tayvan, 5G konusunda Çinli şirketler ile çalışılmaması konusunda yasal düzenlemeler gerçekleştirmişlerdir. Almanya, Huawei'nin donanım ve yazılım güvenliğinin takip edilmesi için özel bir izleme merkezi kurmuştur. Bazı ülkeler ise 5G altyapılarının çekirdeği için Huawei'yi tercih etmezken altyapının sadece asli olmayan kısımlarında şirketin hizmet vermesine izin vermektedir. Örneğin İngiltere, Huawei'nin içerisinde bulunduğu yüksek riskli hizmet sağlayıcıların nükleer santral ve askeri tesisler gibi hassas noktalarda faaliyet gösteremeyeceğini, bu şirketlerin piyasa payının ise % 35 ile sınırlandırılacağını kabul etmektedir. İngiltere, bu kararını içerisinde İngiliz istihbaratından yetkililerin de bulunduğu bir izleme kurulunun, Huawei ile çalışmanın ülkenin ulusal güvenliğine tehdit oluşturmayacağı şeklindeki ra-

poru sonrasında almıştır. İngiltere'de 2014 yılında oluşturulan bu kurul, bazı güvenlik endişeleri olsa da, Huawei'nin Çin devleti adına casusluk yaptığına dair kanıtın bulunamadığını açıklamıştır (Bond ve Fildes: 2019). İngiltere, Huawei'den Radyo Erişim Şebekesi (RAN) konusunda hizmet alırken güvenlik endişeleri ile diğer bir Çinli firma ZTE ile çalışmama kararı almıştır. ABD ise müttefiklerinden Huawei'nin Batı'daki tedarik zincirinin tamamen kesilmesini talep etmiştir. Daha önce Huawei ile anlaşan İngiltere, ABD'nin baskısı üzerine Huawei ile çalışma politikasını değiştireceğini duyurmuştur. İngiltere, ulusal güvenlik gerekçesiyle 2020'den sonra tüm mobil operatörlerin, Huawei'nin 5G radyo ürünlerini satın almasını yasaklamıştır. İngiltere, operatörlerin 2027'ye kadar Huawei kitlerini ağlarından çıkarmaları gerektiğini de duyurmuştur. İsviçre ve Avrupa Birliği ise ABD'nin çağrılarına karşı 5G teknolojisi konusunda Huawei ile çalışacakları konusunda kararlar açıklamışlardır.

ABD, Çinli Huawei gibi yabancı şirketlere karşı kısıtlayıcı düzenlemelere giderken Amerikalı teknoloji şirketleri de zaman zaman yönetimin politikasına paralel kararlar alabilmektedir. Örneğin Microsoft, ABD'nin ticaret ambargosu çerçevesinde 2009'da Messenger uygulamasını Küba, İran, Sudan, Kuzey Kore ve Suriye'de erişime kapatmıştır. (Arsene, 2016). Çin ile süren ticaret savaşı döneminde kullanıcı verilerini sızdırma ihtimali gerekçesiyle ABD'li şirketlerin Huawei ürünlerini satın alması yasaklanmıştır. Donald Trump'ın başkanlığı dönemindeki bu yasak sonrası Qualcomm, Broadcom gibi mikroçip şirketleri Huawei'ye ürün satmayı durdurduklarını açıklamışlardır. (King vd., 2019). Bir başka Amerikalı teknoloji şirketi Google, Android uygulamalarını Huawei telefonlarının son modellerinde kullandırmayacağını duyurmuştur. Bu karar sonrasında Huawei, akıllı telefonları için kendi yazılımını devreye sokma kararı almıştır. Şirketin piyasaya yeni çıkan akıllı telefonlarında Google servisleri yerine Huawei Mobil Servisleri (HMS) yer almıştır (Doffman, 2020). Huawei'nin uygulama marketi AppGallery de, şirketin akıllı telefonlarında resmi bir uygulama dağıtım platformu olarak yer almaktadır.

5G teknolojisi konusunda ABD'nin Huawei kadar başarılı bir şirketi bulunmamaktadır. ABD, bu nedenle 5G konusunda dünyada sadece Huawei'ye bağlı bir sistemin kurulmasını engellemeye çalışmaktadır (Lau, 2020). Ancak ABD tarafından Huawei'ye karşı çıkarılan engeller şirketin kendisini teknolojik olarak daha da geliştirmesine yol açmaktadır. Ayrıca 5G ve diğer hizmetler konusunda ABD'nin öncülük ettiği sınırlamalar Huawei'nin Çin devleti tarafından daha fazla desteklenmesi ihtimalini ortaya çıkarmaktadır. Nitekim ABD, Çinli özel şirketlerin karlılıklarını artırmaları için devletin büyük süb-

vansiyonlar verdiğini savunmaktadır. 2016 yılında ABD Kongresine sunulan bir raporda, Huawei'nin devlet bankaları tarafından "ulusal şampiyon" sıfatıyla büyük meblağlar ile fonlandığı belirtilmektedir. Raporda yine Çin'in ülkeye yatırım yapmak isteyen Amerikalı şirketleri teknoloji transferine zorladığı öne sürülmektedir. ABD Kongresine sunulan raporda Çin'in, Amerikalı şirketlerin ticari sırlarının elde edilmesini desteklediği iddiaları da yer almaktadır. (Findings of the invenstigation, 2018). Ancak ABD'nin kendisi de geçmişte birçok sektöre devlet fonları, yatırımlar, teşvikler, sübvansiyonlar ve vergi kolaylıkları ile destek olmuştur. ABD'de uzay teknolojisinde, savunma sanayinde normal zamanlarda uygulanan destekler 2008 krizi gibi ekonomik zorluk dönemlerinde bankacılık gibi çok daha farklı sektörlere genişlemiştir.

3.3. 5G Jeopolitiği

Huawei ile ABD'nin 5G konusundaki rekabeti dünyada siyasal olarak bölünmüş teknoloji alanlarının ortaya çıkmasına neden olmaktadır. Çin, 5G teknolojisi ile adeta dijital bir İpek Yolu kurma girişimi içerisindedir. 5G jeopolitiği olarak ifade edilebilecek bu yaklaşım, siyasi rekabet ve mücadelenin hatta soğuk savaşın teknoloji alanındaki bir yansıması olarak yorumlanmaktadır (Donahue, 2019). ABD'nin Asya'daki müttefikleri, Huawei ile çalışmama kararları alıp şirketin ürünlerine kısıtlamalar getirmektedirler. Çin ise 5G teknolojisi ile Avrupa Birliği, Ortadoğu, Afrika, Güneydoğu Asya ve Latin Amerika'da projeler gerçekleştirmektedir. Örneğin Afrika Birliği, verilerin çalındığı yönündeki iddialara rağmen Mayıs 2019'da Huawei ile 5G, yapay zeka ve bulut teknolojisi konusundaki sözleşmesini yenilemiştir. Huawei, Afrika Birliği'nin verilerini çaldığı yönündeki iddiaları bir açıklama ile yalanlamıştır (Statement on Huawei's work, 2020). Hatta şirket kendisine dönük casusluk iddialarına karşı güven tazelemek adına küresel siber güvenlik ekibinin başına İngiltere hükümetinde 7 yıl boyunca enformasyon biriminin sorumluluğunu yapan John Suffolk'u getirmiştir (Mascitelli ve Chung, 2019).

Huawei, 5G konusunda neredeyse tüm ihtiyaçları karşılayabilen bir şirket olmasının yanında dünyanın en büyük mobil telekomünikasyon altyapı tedarikçisidir. Huawei, diğer servis sağlayıcılarla karşılaştırıldığında Avrupa'da fiyat rekabetinde öne çıkmaktadır. Avrupa'da 5G konusunda imzalanan sözleşmelerin yarısından fazlası Huawei ile yapılmış durumdadır (Donahue, 2019). Hollanda telekomünikasyonda % 60'lık fiyat avantajı nedeniyle Huawei'yi tercih ederken, 4G ve 4,5G teknolojisinde dünyanın yarısı Huawei altyapısını kullanmaktadır. Avrupalı şirketlerin Huawei altyapısından vazgeçmeleri halinde milyarlarca dolarlık kayıplarının söz konusu olabileceği tahmin edilmektedir. Avrupa'nın telekomünikasyon altyapısının yaklaşık %

50'sinin Çinli firmalar tarafından sağlandığı hesaplanmaktadır (Triolo, 2020). Avrupa'daki bu altyapıyı yok sayarak farklı şirketlere yönelmek ülkeler için hem ek bir maliyet hem de 5G projelerinin ertelenmesi anlamına gelebilmektedir.

ABD, fiyat anlamında rekabetçi olan Huawei ürünlerini kullanan müttefiklerini istihbarat paylaşımını kesmek ile tehdit etmektedir. Ancak Avrupa ülkelerinin çoğunluğu Asya-Pasifik'te doğrudan güvenlik çıkarları olmadığı için Çin'i stratejik bir rakip ve tehdit olarak değerlendirmemektedir (Brauner, 2013). Çoğu Avrupa ülkesi, Çin ile teknoloji dahil ekonomik ilişkilerini geliştirirken Çin'in tehdit olarak algılanmamasında coğrafi uzaklık bir etken olarak ifade edilmektedir. Avrupa Birliği, Çin yerine coğrafi olarak kendisine daha yakın olan Ortadoğu, Kuzey Afrika ve Rusya'yı güvenlik tehdidi olarak algılamaktadır. ABD, Huawei'nin İran'a ambargo kararını da ihlal ettiği görüşündedir. Kanada, Aralık 2018'de ABD'nin talebi üzerine ABD'nin İran'a karşı ticaret yaptırımlarını ihlal ettiği şüphesiyle Huawei CFO'su Meng Wanzhou'yu tutuklamıştır. Meng, ABD'nin İran'a yönelik yaptırımlarını delme, yolsuzluk ve teknoloji hırsızlığı gibi suçlamalar nedeniyle Vancouver havaalanında gözaltına alınmıştır. Huawei'nin kurucusunun kızı ve şirketin Mali İşler Direktörü Meng Wanzhou, daha sonra 10 milyon Kanada doları kefaletle serbest kalmıştır (Sherlock and Bilefsky, 2020).

3.4. Siber Güvenlik

Telekomünikasyon kavramı ekonomi ve siyaset ile doğrudan bağlantısı nedeniyle devletler için bir ulusal güvenlik meselesi olarak değerlendirilmektedir (Devi, 2019). Bilgi ve iletişim teknolojileri ile ülkelerin askeri ve stratejik üsleri kontrol edilebilmektedir. Ülke güvenliği ve ticaret ile ilgili birçok görüşme bu telekomünikasyon altyapısı üzerinden gerçekleştirilmektedir. Bir enerji santralinin şebekesi ile ülkedeki sağlık sistemine ait bilgilerden ticari sırlara kadar her şey bu bilgi ve iletişim ağları üzerinden yürütülmektedir. Devletlere dönük saldırılar doğrudan askeri ya da stratejik öneme sahip tesisleri fiziki olarak yok etmek yerine bu ağlar üzerinden gerçekleştirilebilmektedir. (Lowe, 2006). Yapılan siber saldırılar kimi zaman söz konusu tesisin fiziki olarak yok edilmesi kadar etkili olabilmektedir. Siber altyapı sistemlerine yapılan saldırılar sonrası yaşanan aksaklıklar can kaybı ve ekonomik kayıpların yanında ulusal prestij, moral ve güvenin yıkılmasına da neden olabilmektedir (Farwell, 2012).

İnternet bir ulusal güvenlik meselesi olarak kabul edildiğinden bu yana devletlerin bu alanda zorlayıcı araçlar ve sürpriz durumlara karşı yetenekler geliştirmesi beklenmektedir (Mueller vd.,2013). Siber saldırıların, ekonomik

amaçlar ile siyasi amaçların birleştiği operasyonlar haline dönüşme ihtimali bulunmaktadır. ABD'li güvenlik yetkilileri, 2009'da Çin ve Rusya'dan ajanların ABD'nin güç şebekesinin kırılganlıklarını araştırdığını öne sürmüştür. Bu iki ülkeden ajanların ABD'de elektrik sisteminde kesintiye yol açabilecek bir yazılım programını çalıştırdıkları iddia edilmektedir (Gorman, 2009). 2012 yılında dünyanın en büyük petrol üreticisi Suudi Aramco'nun bilgisayarlarına yapılan Shaaman virüsü saldırısı, etki açısından kayda değer örneklerden birisi olarak gösterilmektedir. Bu virüs saldırısında Aramco'nun bilgisayarlarının üçte birine denk gelen yaklaşık 30 bin bilgisayar kullanılamaz hale gelmiştir (Tarter, 2015). Aramco'nun, saldırı öncesi hali ile petrol üretimine dönmesi yaklaşık 5 ay sürmüştür. Suudi Aramco'nun güvenlik yetkilileri bu saldırının arkasında İran'ın olduğunu iddia etmişlerdir (Easttom, 2018). İran ile siyasi gerilim yaşayan Suudi Arabistan'ın enerji şirketi Aramco'ya yapılan siber saldırının, 2010 yılında İran'ın Natanz nükleer tesislerindeki bilgisayarlara yapılan saldırının bir misillemesi olduğu tahmin edilmektedir. ABD ve İsrail'in arkasında olduğu iddia edilen ve Stuxnet isimli yazılım ile gerçekleştirilen bu siber saldırı ile İran'ın nükleer programının yaklaşık 2 yıl gecikmeye uğradığı değerlendirilmektedir (Finnemore ve Hollis, 2016). Stuxnet virüsünün petrol ve doğalgaz boru hatları, petrol platformları, elektrik santralleri ve diğer sanayi kuruluşlarını kontrol etmekte kullanılan Alman Siemens şirketinin programını hedeflediği iddia edilmiştir. Siber saldırı uzmanları, Stuxnet virüsü ile gerçekleştirilen saldırının devlet desteği olmadan yapılamayacağını ifade etmişlerdir (Lachow, 2011).

ABD'de Çin kaynaklı siber operasyonlara dair çeşitli raporlar yayınlanmaktadır. Şubat 2013'te Amerikalı siber güvenlik firması Mandiant, Çin ordusuna bağlı bilgisayar korsanlarının aktivitelerini detaylı bir şekilde rapor etmiştir. Mandiant raporunda, bilgisayar korsanlarının fikri mülkiyet hırsızlığı yaptıkları ve Amerikan devlet kurumlarını hedef aldıkları iddia edilmektedir. ABD Temsilciler Meclisi İstihbarat Komitesi, 2012 yılındaki raporunda Huawei ve ZTE'yi yolsuzluk ve rüşvet ile suçlayarak Federal Soruşturma Bürosu'ndan (FBI) araştırma talep etmiştir (Dobson, 2017). Kamuoyuna sızan bir FBI raporuna göre, Çin'in 30 bin kişilik bir siber ordusu bulunmaktadır. Aynı rapora göre Çin'de siber operasyonlar için özel sektörden kiralanan 150 bin kişilik bir siber casus ekibi yer almaktadır (Hjortdal, 2011). Amerikan Savunma Bakanlığı, Çin hükümetinin bilgisayar korsanlarına yardım ettiğine dair iddiaları dile getirmiştir (Wang, 2016). Ancak ABD'deki iddiaların yanında ABD Kongresi ve Beyaz Saray tarafından yürütülen resmi soruşturmalarda Huawei'nin Çin devleti adına casusluk yaptığına ilişkin kesin kanıtlara ulaşılamamıştır (Iasiello, 2016).

ABD ile Çin arasında siber alanda karşılıklı güvensizlik oldukça yüksektir (Kolton, 2017). Çin, ülkesinin siber saldırıların en büyük kurbanlarından biri olduğunu öne sürmektedir. Çin Savunma Bakanlığı, ülkesine karşı yaşanan bilgisayar korsanlığı saldırılarının çoğunun Amerikan kaynaklı olduğunu iddia etmektedir. Çin, önlem olarak resmi kurumlarda Windows sistemleri yerine giderek daha fazla Linux sistemlerini kullanmayı tercih etmektedir. Ancak bu dönüşümün 3 ila 10 yıl arasında süreceği tahmin edilmektedir (Artashyan, 2020). Çin yetkilileri bu önlemler ile ABD istihbaratının kendi bilgisayarlarına erişimini engellemeyi amaçlamaktadır. Çin'de 1 milyon IP adresinin ülke dışından kontrol edildiği ifade edilmektedir (Ball, 2011). Çin, ayrıca Amerikan Ulusal Güvenlik Ajansı'ndan (NSA) Huawei'ye dönük casusluk girişimlerinin açıklanmasını talep etmektedir. NSA'ye dönük iddialar Çinli şirketler ile sınırlı değildir. NSA'in, Dünya Bankası, Uluslararası Para Fonu (IMF), Avrupa Komisyonu ile birlikte Brezilya'nın en büyük petrol şirketi Petrobras'ı da izlediği ortaya çıkmıştır (Watts, 2013). ABD ise siber operasyonlarının ulusal güvenlik kaygısı ile gerçekleştirildiğini ve Amerikan şirketlerine dönük ticari bir avantaj sağlama amacının olmadığını ifade etmektedir.

ABD'de resmi yetkililer arasındaki iletişim dahil ülkedeki bütün sistem ticari ve özel telekomünikasyon altyapısına bağlıdır. Bu nedenle siber altyapıyı korumak için ABD hükümeti özel sektör ile işbirliği yapmak zorundadır. ABD, bu alanda bir Siber Komutanlığa sahip olsa da ülkenin kritik siber altyapısının % 90'ı özel sektöre aittir (Farwell, 2012). ABD'de iletişim güvenliği konusu ülke içi ile de sınırlı değildir. Örneğin ABD askerlerinin olduğu Irak'taki telekom altyapısının neredeyse tamamı Huawei tarafından sağlanmaktadır. ABD Dışişleri Bakanlığına göre, 2004 yılından bu yana şirketin Irak'ta imzaladığı altyapı sözleşme sayısı 600'ü geçmiş durumdadır (Waterman, 2011). Irak'ta askerlerin güvenlik için kullanılan güvenlik kamera sistemleri de Huawei ile gerçekleştirilen işbirliği sayesinde sunulmaktadır (China's Huawei helps, 2020). ABD, Irak'ta 2003'teki işgal sırasında kullandığı silahların % 68'ini uydu teknolojileri aracılığı ile yönlendirmiştir, bu oran 1990'daki Körfez Savaşı'nda yalnızca % 10'dur (Ünal, 2019). Dolayısıyla ABD için teknoloji güvenliği meselesi ve Huawei tehdidi ile mücadele ülke içi ile sınırlı kalmamaktadır. ABD askeri varlığının olduğu birçok ülke başta olmak üzere, ABD'nin çıkarlarının olduğu Avrupa'dan Afrika'ya kadar çok geniş bir mücadele alanı söz konusudur.

Avrupa'da birçok ülke 5G konusunda Huawei ile çalışma kararı alırken konu siber güvenlik meselesi olarak da değerlendirilmektedir. Siber güvenlik ile bilgi ve iletişim teknolojisi standardizasyonunda ortak bir politika geliştirmeyi hedefleyen Avrupa Birliği, 2004'te AB Siber Güvenlik Ajansı olan

ENISA'yı kurmuştur. ENISA, üye ülkelere siber güvenlik tehditleri ve saldırıları ile mücadelede destek vermektedir (ENISA, 2021). Mart 2019 tarihinde AB Parlamentosu'nda onaylanan Avrupa Birliği Siber Güvenlik Kanunu, çevrimiçi hizmetlerin ve tüketici cihazlarının siber güvenliğini artırarak, siber güvenlik sertifikası için bir AB çerçevesi oluşturmaktadır (Deloitte, 2020). Ancak tüm bu ortak çabalara karşın Avrupa Birliği'nde ulusal güvenlik politikaları üye ülkelerin nihai kararlarına bırakılmaktadır. Başta Almanya olmak üzere Avrupa ülkeleri meseleyi ulusal çıkar perspektifi ile birlikte ekonomik bağlamda da değerlendirmektedir. Çin, Avrupa'nın önemli ticaret ortaklarından birisidir. Dolayısıyla Avrupa'da Huawei'ye dönük olası sınırlamalara karşı Çin'in misillemede bulunma ihtimali söz konusudur. Almanya'nın Huawei'ye dönük olası bir yasaklama girişimine karşı Çin, üstü kapalı bir şekilde ülkesinde satılan Alman otomobilleri ile ilgili benzer kararlar alabileceğini ima etmiştir (Bennhold and Ewing, 2020).

3.5. ABD'nin Huawei Önlemleri ve Şirketlere Etkisi

ABD, müttefiklerini de ikna ederek Huawei ürünlerine olan talebin önüne geçmeye çalışmaktadır. ABD'nin Huawei ile mücadele politikası konusundaki diğer seçenekler ise ya ülke içerisinden ona karşı bir rakip çıkarmak ya da küresel bir yabancı oyuncuyu ona karşı desteklemektir. 1960'larda Sovyetler ile yaşanan uzay rekabetinde olduğu gibi Çin ile mücadele için ABD'de telekomünikasyon sektöründe devlet yatırımlarının artırılması talep edilmektedir (Donahue, 2019). ABD'de nüfus yoğunluğu düşük olan kırsal alanlarda telekomünikasyon sektörü Finlandiyalı Nokia ve İsveçli Ericsson'a bağlıdır. Bu bölgelerde çalışan şirketler % 25 oranında Huawei ekipmanlarını kullanmaktadır. Nokia ve Ericsson'un yaşadığı finansal sorunların ardından Huawei'nin pazar payı bu iki şirketin pazar payının üzerine çıkmıştır. Yalnızca pazar payı olarak değil teknolojik olarak da Huawei'nin bu iki şirkete karşı üstünlüğü ifade edilmektedir. Huawei, her yıl 15 milyar doların üzerinde araştırma ve geliştirme harcaması yapmaktadır. Nokia ve Ericsson'un toplam ar-ge harcaması ise yaklaşık 10 milyar dolarda kalmaktadır. Huawei'nin dünya genelinde 80 bin ar-ge çalışanı bulunurken bunun tüm çalışanlarına oranı % 45 olarak hesaplanmaktadır (Artashyan, 2019). Huawei'nin 23 bin 500'den fazla ödüllü patenti bulunurken bunların % 90'ı teknolojik bir icat olarak tanımlanmaktadır (Tao ve Chunbo, 2015).

ABD, Çinli şirketlerin ülkedeki teknoloji sanayilerine yatırımına da kuşku ile bakmaktadır. Bu nedenle Başkan Gerald Ford'un kararı ile 1975 yılında oluşturulan, ABD Yabancı Yatırım Komitesi (CFIUS) yabancı yatırım girişimleri ile ilgili değerlendirmeler yapmaktadır (Farwell, 2012). Çinli

şirketler sadece ABD'de değil dünyanın farklı bölgelerinde de engeller ile karşılaşmaktadır. Çin'in 2005-2015 yılları arasındaki 432 yurtdışı doğrudan yatırım girişiminin 22'si siyasi engeller ile karşılaşmış ve başarısız olmuştur. Bu 22 başarısız yurtdışı doğrudan yatırım girişiminin 9'u ABD tarafından engellenmiştir (Wang ve He, 2019). ABD, Çinli şirketlerin girişimlerini bir güvenlik meselesi olarak değerlendirirken Çinli şirketlerin Amerikalı şirketlere dair satın alma ve yatırımlarının Çin devletinin sistematik sanayi planları çerçevesinde olduğunu savunmaktadır. Çinli yatırımcılar yurtdışındaki yabancı şirketlerden pay aldıktan sonra ürünlerin Çin'de üretimi ve dağıtımını talep etmektedirler. ABD, Çinli şirketlerin satın alma girişimlerindeki hedeflerinin önemli teknolojik bilgilere ulaşmak olduğunu iddia etmektedir. ABD, bu kuşkuya dönük sınırlama ve önleme girişimlerine başvurmaktadır. Nitekim Huawei'nin 2008 yılında 3COM, 2010 yılında internet yazılım şirketi 2Wire ve aynı yıl Motorola'nın telsiz ekipmanları işini satın alma girişimi ABD'de engeller ile karşılaşmıştır. Huawei'nin 2011 yılında 3Leaf Systems isimli finansal açıdan zor durumdaki bir teknoloji şirketini satın alma girişimi ABD Kongresinden gelen tepkiler sonrası gerçekleşememiştir (Wang ve He, 2019). Washington yönetimi yalnızca ABD şirketleri değil Huawei'ye hizmet sunan diğer yabancı şirketlerin de önünü kesmek istemektedir. Beyaz Saray, Huawei'ye yarı iletken ürünler sunan Tayvanlı TSMC ve Güney Koreli Samsung'a da yaptırım uygulayabileceğini duyurmuştur (Davis ve Ferek, 2020). ABD'nin Çinli teknoloji şirketlerine karşı yaklaşımı Huawei ile sınırlı değildir. ABD, Çinli bir diğer telekomünikasyon devi ZTE şirketine çip satışlarını durdurma kararı almıştır. Dönemin ABD Başkanı Donald Trump, Mayıs 2019'da Huawei'nin de aralarında olduğu yaklaşık 70 şirketi kara listeye almıştır. Kararla Huawei, ABD'de ürün satamazken ABD'de üretilen ürünlerden ve hizmetlerden de Çinli bu şirketlerin yararlanamayacakları açıklanmıştır (Shepardson and Freifeld, 2020). Haziran 2019'da Japonya'da yapılan G-20 Zirvesi sonrasında ise Trump, Çin ile yaptıkları görüşmeler sonrasında Amerikalı şirketlerin ulusal güvenlik gerekçesiyle Huawei'ye donanım satmasına getirilen kısıtlamanın gevşetileceğini duyurmuştur. Bu yumuşama ile birlikte Microsoft, Huawei'ye yazılım satmak için izin almıştır (Phelan, 2019).

Mayıs 2020'de Huawei ile ilgili yeni yaptırım kararları açıklayan ABD, şirketin ABD ihracat sınırlama kurallarındaki boşluklardan faydalanmasını engellemeyi amaçlamaktadır. Karar ile birlikte ABD teknolojisi ve yazılımlarını kullanarak üretilen yarı iletken çipleri Huawei'ye satan yabancı firmalar için sıkı ihracat kısıtlamaları getirilmiştir. ABD teknolojisi ile üretilen ürünleri Huawei'ye satmak isteyen firmalar, artık ABD'den lisans almak zorunda kalmaktadırlar. ABD yönetiminin bu kararının ardından dünyanın en büyük

çip üreticisi Tayvanlı TSMC, Huawei'den aldığı tüm siparişleri durdurma kararı almıştır. Çin ise ABD'nin aldığı karar ile kendilerini teknolojik bir soğuk savaşa sürüklediğini savunmaktadır (Qingqing ve Qiaoyi, 2020).

ABD'li birçok teknoloji şirketi gelir ve karlılık açısından Çin'e bağımlıdır ve ABD yönetiminin yaptırımları bu şirketleri de olumsuz etkilemektedir. Intel'in gelirinin % 20'si, Qualcomm'un gelirinin ise % 40'ı Çin'e gerçekleşen satışlardan kaynaklanmaktadır. ABD'li NeoPhotonics isimli şirketin gelirinin % 49'u sadece Huawei'ye yapılan satışlardan gelmektedir (Donahue, 2019). Dolayısıyla ABD'nin Huawei ve Çinli şirketlere olan engelleyici tavrı, ABD'li teknoloji şirketlerini de gelir açısından olumsuz etkileyebilmektedir. Engellemeler öncesi Huawei'nin ABD'li teknoloji şirketlerine olan ödemesi yıllık yaklaşık 10 milyar dolar olarak hesaplanmıştır. ABD hükümetinin yaptırım kararlarına rağmen Intel ve Microsoft gibi teknoloji şirketleri Huawei'ye hayati ekipmanları satma konusunda isteklidir. ABD'li şirketler, kendi gelirlerini ve araştırma geliştirme bütçelerini olumsuz etkileyeceğini savunarak Huawei'ye dair yasaklara karşı çıkmaktadırlar.

ABD'nin Huawei'ye dönük güvenlik kaygıları ile birlikte gelen sınırlama politikasına rağmen şirket büyümesini sürdürmektedir. Ancak ABD yaptırımlarının etkisi ile şirketin net kar ve gelir rakamlarındaki artış oranı 2019'da azalmıştır. Huawei'nin kurucusu Ren Zhengfei, ABD'nin yaptırımları nedeniyle şirketin yıllık gelir kaybının 30 milyar doları bulabileceğini söylemiştir (Gao ve Wu, 2020). Huawei'nin 2019 yılı net karındaki artış % 5,6 olurken bu son üç yıla nazaran bir yavaşlamaya işaret etmektedir. Huawei'nin gelirleri ise 2019 yılında bir önceki yıla benzer şekilde % 19 artışla 123 milyar dolar olmuştur. ABD'nin sınırlamaları ve müttefiklerine dönük bu yöndeki çağrıları sonrası 2019 yılında şirketin gelirlerini daha çok Çin'den elde ettiği görülmüştür. Japonya ve Avustralya'da Huawei'ye dönük yaptırımlar sonrasında 2019 yılında şirketin Asya-Pasifik bölgesi gelirleri % 13,9 oranında düşmüştür. Huawei, Avrupa, Ortadoğu, Afrika (EMEA) ve Amerika gibi pazarlarda Google'ın uygulama yasağı sonrası Güney Koreli rakibi Samsung ile rekabette zorlanmaya başlamıştır. ABD yaptırımlarının olmadığı 2018 yılında ise Huawei'nin EMEA bölgesi satışları % 24,3 Amerika bölgesi satışları % 21,3 ve Asya Pasifik bölgesi satışları da % 15,1 artmıştır (Gao and Wu, 2020). 2020 yılında ise ABD yaptırımlarının Huawei'nin geliri üzerindeki etkisi çok daha net görülmektedir. 2020'de Huawei'nin geliri yalnızca % 3,8 oranında artmıştır. 2020 yılı bilançosunda COVID-19 pandemisinin olumsuz etkisi de hissedilirken şirket yalnızca Çin'de gelir büyümesi kaydetmiştir. 2020 yılında Huawei'nin net karındaki artış % 3,2 olarak kaydedilmiştir (Kharpal, 2021).

4. Çin'in Siber Egemenlik Anlayışı

"Huawei tehdit mi?" sorusu aslında ülkeler arasındaki teknoloji rekabeti nedeniyle pek çok şirket için de dillendirilebilmektedir. Mevcut soru, "Facebook, Google, Instagram, Twitter bir tehdit mi?" şeklinde de sorulabilmektedir. Nitekim Batılı teknoloji şirketleri, Çin için önlem alınması gereken ciddi bir endişe kaynağı haline gelmektedir. Çin, ülkesi için siber güvenliği, rejimin devamlılığı ve ulusal güvenlik meselesi olarak görmektedir. Hatta siber egemenlik kavramı ile ulusal sınırlar içerisinde teknoloji ve internette düzenleme yapma ve yasaklama gibi hakları meşrulaştırmaktadır. Çin'de siber egemenlik kavramı, ABD hegemonyasının siber alandaki yayılmacılığına bir karşı duruş olarak kabul edilmektedir (Arsene, 2016). İnternetin ilk dönemlerinde olan özgürlükçü yapısı ile bu dönemin farklı olduğu belirtilerek bu alanda Siber Vestfalya olarak adlandırılan devlet egemenliği ve kurallarının geçerli olduğu bir sürece geçildiği değerlendirilmektedir (Demchak, 2016).

Çin, kendisine dönük suçlamalara eski ABD Ulusal Güvenlik Ajansı (NSA) çalışanı Edward Snowden'ın ifşaları ile yanıt vermektedir. Snowden'ın 2013'te ifşa ettiği belgeler, NSA'in Amerikalı teknoloji şirketlerinin topladığı tüm özel iletişim verilerine erişebildiğini göstermiştir. Söz konusu belgeler ayrıca yabancı ülke vatandaşlarına ait tüm internet yazışmalarının mahkeme izni olmaksızın bilgi toplamak için NSA tarafından kullanılabildiğini ortaya çıkarmıştır. ABD'nin PRISM isimli program aracılığıyla Google, Microsoft ve Yahoo'yu kullanarak internet iletişimini izlediği anlaşılmıştır (Arsene, 2016). İfşa edilen belgeler ayrıca NSA'in ABD'nin organize ettiği gizli birimler yoluyla yabancı şirketler ve ülkelerin hükümet binalarını gizlice dinlediğini ve kayıtlar tuttuğunu göstermiştir.

ABD, Huawei'yi Çin istihbaratı ile bağlantılı olmak ile suçlarken NSA, 2014 yılında Huawei'nin bilgisayar hizmet sunucularına karşı siber saldırı gerçekleştirmiştir (Finnemore ve Hollis, 2016). NSA'in bu operasyonda Çin ordusu ile Huawei arasındaki olası bağlantıyı araştırdığı ortaya çıkmıştır. NSA'in ayrıca Huawei'nin üst düzey yöneticileri arasındaki iletişim kayıtlarını elde ederek şirketin teknolojik bilgilerini hedeflediği de sızan belgelerde yer almaktadır (Dunham: 2014). Huawei, ABD'nin 5G konusundaki engellemesinin de NSA'in izinsiz bilgi toplama faaliyetleri ile ilgili olduğunu iddia etmektedir. Huawei CEO'su Gua Ping, ABD'nin istihbarat faaliyetlerine ters düştüğü için şirketin dünyada kurduğu 5G altyapılarına karşı çıkıldığını savunmaktadır (Doffman, 2019). Rus siber güvenlik şirketi Kaspersky, ABD'nin Çin, Rusya, Pakistan, Afganistan ve İran'da yerleşmiş bilgisayarlar ve ağlar ile kalıcı olarak yerleşmiş şekilde gözetim faaliyeti yürüttüğünü rapor

etmektedir (Yuen, 2015). Çin bu nedenle 2014 yılında denetim için bankalarının yurtdışından satın aldığı yazılım ve donanımların gizli güvenlik kodlarını talep etme kararı almıştır. Çin'in yerli teknoloji hamlesi sadece ekonomik bir hedef değil yabancı şirketler ile ilgili kuşku nedeniyle aynı zamanda bir ulusal güvenlik hedefi ve politikasıdır. Çin, Amerikalı Apple dahil yabancı teknoloji ürünlerini güvenlik kaygıları ile incelemeye almaktadır. Huawei'nin ABD'de karşılaştığı zorluklara karşı Çin de Apple'ın ülkesindeki operasyonlarına karşı adeta misilleme yaklaşımı ile baskı kurmaktadır (Dobson, 2017).

Fikri mülkiyet hakları konusundaki ABD'deki rahatsızlık, Çinli otoritelerin ülkeye yatırım yapacak yabancı şirketlere teknoloji transferi yapmaları konusunda baskı kurdukları savına dayanmaktadır. ABD Ulusal Güvenlik Ajansı'nın eski direktörü Keith B. Alexander, fikri mülkiyet hakları kayıplarını insanlık tarihinin en büyük varlık transferi olarak yorumlamaktadır (Demchak, 2016). ABD, Çin kanunlarına göre yabancı şirketlerin pazara sadece Çinli yerel şirketler ile ortak girişim kurarak girebileceğini iddia etmektedir. ABD'nin iddiasına göre bu zorunluluk, Çin'in ABD'li şirketlerin teknolojilerine erişmesine imkan sağlayabilmektedir. Ancak fikri mülkiyet hakları konusundaki tüm suçlamalara karşın Çin, Uluslararası Para Fonu (IMF) rakamlarına göre dünyanın en çok lisans ücreti ödeyen dördüncü ülkesi konumundadır. Çin'in telif hakkı ödemeleri ve fikri mülkiyet hakları konusundaki lisans ödemeleri son on yılda dört katına yükselmiş durumdadır (Lo, 2019). Çin'in Mart 2019'da yasalaştırdığı Yabancı Yatırımlar Kanunu, yabancı yatırımcıların Çin pazarına girişte karşılaştıkları zorlukları giderme çabalarını içermektedir. Buna göre yabancı yatırımcılar negatif listeye düşmeyen yatırım projelerinde Çinli benzerleri ile aynı muameleye tabi tutulacaktır. Taahhüt edilen bu yaklaşıma göre Çin, yabancı yatırımcıların fikri mülkiyet haklarının korunması için güvence vermektedir. Nitekim ABD-Çin Ticaret Anlaşmasının birinci fazının ilk bölümü de konunun önemine atfen fikri mülkiyet hakları ile başlamaktadır. Çin, fikri mülkiyet haklarına saygı duymayı kabul ederken ticari sırlar konusundaki ihlalleri cezalandırma konusunda taahhütlerde bulunmaktadır (Economic and Trade Agreement, 2020).

5. Sonuç

Çin'in uzun vadeli küresel siyasi stratejik hedefleri nedeniyle başta Huawei olmak üzere Çinli teknoloji şirketlerinin girişimlerine dünyada kuşkuyla bakılmaktadır. Bu endişenin en yüksek olduğu yer olan ABD, ülkesindeki Çin yatırımlarını, şirket satın alma ve birleşmelerini ulusal güvenlik açısından da sorgulamaktadır. ABD, Huawei'yi fikri mülkiyet hakları ihlali ve İran yaptırımlarını delmek gibi suçlardan sorumlu tutmaktadır. Çin'in büyük yatırımla-

rı, ABD'de sadece bir özel sektör girişimi olarak değil Çin devletinin hedefleri doğrultusunda adımlar olarak yorumlanmaktadır. Dolayısıyla Huawei başta olmak üzere Çin kökenli teknoloji şirketlerinin ABD'deki yatırımları Truva atı benzetmesi ile bir finansal ve teknolojik işgal tehdidi olarak değerlendirilmektedir (Flamini, 2014).

Çin hükümetinin Huawei'ye olan desteği bir sır değildir. Nitekim Çin hükümeti, başta ABD olmak üzere şirkete dönük engellemelere olan tepkisini açıkça dile getirmektedir. Hatta Huawei'ye dönük yasaklamalara gerek teknoloji sektörü gerek başka sektörler ile karşılık vereceği mesajını iletmektedir. Örneğin Amerikalı General Motors (GM) şirketi, yaklaşık 3 milyon araç satışı ile Çin'in en büyük ikinci yabancı otomotiv şirketi konumundadır. GM, kendi ülkesinden daha fazla otomobil satışını Çin'de gerçekleştirmektedir. Dolayısıyla Huawei'ye dönük ABD yaptırımları sadece Huawei'ye mal satan Amerikalı teknoloji şirketlerini değil, başka sektörlerden şirketleri de olumsuz etkileme potansiyeline sahiptir.

ABD, Huawei'ye siber casusluk ve güvenlik kaygıları ile yaklaşırken Batılı müttefiklerinden de aynı yaklaşımı beklemektedir. ABD'nin Huawei ve ZTE gibi Çinli telekomünikasyon şirketleri ile sürdürdüğü mücadele teknolojik soğuk savaş nitelendirmesini alsa da dünya henüz bu konuda gerçek soğuk savaş dönemindeki kadar kutuplara ayrılmış değildir. Başta Almanya olmak üzere Avrupalı devletler ekonomik gerekçeler ile Huawei ile çalışmayı sürdürmektedirler. 1980-2010 yılları arasında Çin'in teknoloji ithalatının yaklaşık yarısı Avrupa'dan temin edilmiştir (Brauner, 2013). O dönemlerde "Almanya'nın büyük pazarlara, Çin'in de teknolojiye ihtiyacı var" düşüncesi ile ikili ticaret hızla gelişmiştir. Geçmişteki bu düşünce günümüzde, "5G ile Çin'in yeni ve büyük pazarlara, Almanya'nın ise teknolojiye ihtiyacı var" haline dönüşmüştür.

Fikri mülkiyet hakları, siber casusluk, 5G rekabeti başlıkları ile tartışılan Huawei ile ABD arasındaki gerilim aslında yükselen ve ekonomik olarak güçlenen Çin ile ABD arasındaki mücadelenin bir yansımasıdır. Bu mücadelede taraflar kimi zaman karşı tarafın teknolojik zayıflıklarını ortaya çıkarıp bundan yararlanmak isteyebilir. Hatta siber alandaki mücadelenin bir yansıması olarak karşı tarafın bilgisine ulaştıktan sonra onu manipüle etmeye gayret edebilir (Riikonen, 2019). Ancak iki ülke arasında siber alanda yaşanan bu çatışmanın yakın dönemde sıcak bir savaşa dönüşme ihtimali oldukça azdır. Serbest ticaretin ve küreselleşmenin avantajlarından yararlanarak dünyanın ikinci büyük ekonomisi konumuna ulaşan Çin, ABD ile askeri olarak karşı karşıya gelme niyetinde değildir. Çin, ünlü komutanı Sun Tzu'nun MÖ 6.yüz-

yılda yazdığı eserinde yer aldığı gibi, barışçıl şekilde savaşmadan düşmanı kontrol altına alma stratejisini uygulamaktadır (Tzu, 2000). Çin ordusu da elbette ülkenin ekonomik ve teknolojik gelişiminden olumlu etkilenmektedir. Çin ordusu, insansız otonom sistemler, savaş simülasyonları, istihbarat ve veri birleştirme analizi gibi konularda binden fazla Çinli şirket ile işbirliği halinde teknoloji projeleri yürütmektedir (Kennedy, 2019). Ayrıca ülke dışından sağlanan teknoloji transferlerinden Çin ordusu da dolaylı olarak faydalanmaktadır (Brauner, 2013).

Çin ekonomik olarak gelişmeye odaklanırken ABD gibi bir büyük güç olduğunun kabullenilmesini hedeflemektedir. Mesele Huawei'den bağımsız şekilde Çin'in ABD ekonomisi ve hakimiyetini tehdit eder şekilde dünyanın iki numaralı ekonomisi haline gelmesi ile ilgilidir. Üstelik Çin bunu artık sadece ucuz işgücüne dayalı üretim ile değil Huawei gibi yüksek teknolojiyi üreten ve buna liderlik ederek ihraç eden bir yapı ile gerçekleştirmektedir. Çin, Avrupa'dan Afrika'ya ekonomik ve siyasi olarak etki alanını genişletirken ABD ile gerilim yaşanması kaçınılmaz görünmektedir. Dolayısı ile "Huawei bir tehdit mi?" sorusu temelde "Çin, ABD için bir tehdit mi?" sorusunda kilitlenmektedir.

Kaynakça

Acemoğlu, D. ve Robinson, J. A. (2019). Ulusların Düşüşü. 50. Baskı. İstanbul: Doğan Kitap.

Akkemik, K.A. ve Tuncer, B. M. (2019). Çin-ABD Ticaret Savaşları Gölgesinde Çin Sanayi Ve Teknoloji Politikaları. M.Yağcı Ve C.Bakır (Der.), Çin Bilmecesi İçinde (s.75-99). İstanbul: Koç Üniversitesi Yayınları.

Alkhawajah, W. (2019). Huawei: An Information and Communications Technology Company. Journal of it And Economic Development, 10(1),1-10.

Arsene, S. (2016). Global Internet Governance in Chinese Academic Literature: Rebalancing A Hegemonic World Order?. China Perspectives, No. 2 (106), 25-35.

Artashyan, A. (2019). Huawei's R&D Personnel of 80,000 Accounts for % 45 of Total. https://www.gizchina.com/2019/11/04/huaweis-rd-personnel-of-80000-accounts-for-45-of-total/

Artashyan, A. (2019). It Will Take 3-10 Years for Linux to Replace Windows in China. https://www.gizchina.com/2020/05/10/it-will-take-3-10-years-for-linux-to-replace-windows-in-china/

Ball, D. (2011). China's Cyber Warfare Capabilities. Security Challenges, Vol. 7, No. 2, 81-103.

Bennhold, K. and Ewing, J. (2020). In Huawei battle, China Threatens Germany 'Where It Hurts': Automakers. https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html

Bond, D. ve Fildes, N. (2019). UK Intelligence Panel Warns on Huawei Security Flaws. https://www.ft.com/content/8d701096-50ac-11e9-b401-8d9ef1626294

Brand Finance Global 500. (2020). The Annual Report On The World's Most Valuable And Strongest Brands. https://brandfinance.com/wp-content/uploads/1/brand_finance_global_500_2020_preview.pdf

Brauner, O. (2013). Beyond The Arms Embargo: EU Transfers Of Defense And Dual-Use Technologies To China. Journal of East Asian Studies, Vol. 13, No. 3, 457-482.

Davis B. ve Ferek, K.S. (2020). U.S. Moving Forward With Rule To Limit Chips To Huawei. https://www.wsj.com/articles/u-s-moving-forward-with-rule-to-limit-chips-to-huawei-11585261519

Deloitte Avrupa Birliği Siber Kanunu. (2021). https://www2.deloitte.com/tr/tr/pages/risk/topics/cyber-risk/articles/avrupa-birligi-siber-guvenlik-kanunu.html

Demchak, C.C. (2016). "Uncivil And Post-Western Cyber Westphalia: Changing Interstate Power Relations Of The Cybered Age", The Cyber Defense Review, Vol. 1, No. 1, 49-74.

Department of State Summary of the 2018 National Defence Strategy of the United States of America. (2018). https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Devi, S. (2019). Cyber Security In The National Security Discourse. World Affairs: The Journal of International Issues, Vol. 23, No. 2, 146-159.

Dobson, W. (2017). China's State-Owned Enterprises And Canada's Foreign Direct Investment Policy. Canadian Public Policy / Analyse de Politiques, Vol. 43, No. S2, 39-44.

Doffman, Z. (2019). Huawei Claims U.S. Onslaught Is Because Their 5G Technology Prevents Widespread NSA Spying. https://www.forbes.com/sites/zakdoffman/2019/02/28/huawei-the-u-s-is-afraid-we-will-stop-the-nsa-spying-it-has-nothing-to-do-with-china/#f3538e6bc00d

Doffman, Z. (2020). Goodbye Google-Huawei Now Urgently Turns To Apple Instead. https://www.forbes.com/sites/zakdoffman/2020/08/15/huawei-apple-iphone-google-android-update-release-beat-china-ban/?sh=51f16f867cc0

Donahue, T. (2019). The Worst Possible Day. Prism, Vol.8, No.3, 14-35.

Dunham, W. (2014). NSA Infiltrates Servers Of China Telecom Giant Huawei: Report. https://www.reuters.com/article/us-usa-security-china-nsa/nsa-infiltrates-servers-of-china-telecom-giant-huawei-report-idUSBREA2L0PD20140322

Easttom, C. (2018). An Examination Of The Operational Requirements Of Weaponised Malware. Journal of Information Warfare, Vol. 17, No. 2, 1-15.

ENISA, (2021). About ENISA-The European union agency for cybersecurity. https://www.enisa.europa.eu/about-enisa

Farwell, J.P. (2012). Industry's Vital Role In National Cyber Security. Strategic Studies Quarterly, Vol. 6, No. 4, 10-41.

Finnemore, M. ve Hollis, D. B. (2016). Constructing Norms For Global Cybersecurity. The American Journal of International Law, Vol. 110, No. 3, 425-479.

Flamini, R. (2014). Beijing Inc? The Chinese Aren't Coming-They're Here. World Affairs, Vol. 177, No. 4, 71-79.

Gao, Y., Chan E. and Nicola, S. (2020). How Huawei Landed At The Center Of Global Tech Tussle. https://www.bloomberg.com/news/articles/2019-12-17/how-huawei-landed-at-the-center-of-global-tech-tussle-quicktake

Gao, Y. and Wu, D. (2020). Huawei Warns Of 'Pandora's Box' If U.S. Curbs Taiwan Supply. https://www.bloomberg.com/news/articles/2020-03-31/huawei-reports-jump-in-2019-profits-despite-u-s blacklist?utm_source=google&utm_medium=bd&cmpId=google

Gorman, S. (2009). Electricity Grid In U.S. Penetrated By Spies. https://www.wsj.com/articles/SB123914805204099085

Harwit, E. (2007). Building China's Telecommunications Network: Industrial Policy And The Role Of Chinese State-Owned, Foreign And Private Domestic Enterprises. The China Quarterly, No. 190, 311-332.

Hjortdal, M. (2011). China's Use Of Cyber Warfare: Espionage Meets Strategic Deterrence. Journal Of Strategic Security, Vol. 4, No. 2, 1-24.

Hoffman, S. And Kania, E. (2018). Huawei And The Ambiguity Of China's Intelligence And Counter- Espionage Laws. https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/

Holz, C. A. (2018). Industrial Policies And The Changing Patterns Of Investment In The Chinese Economy. The China Journal, Vol.81, 1-55.

Statement On Huawei's Work. (2020). https://www.huawei.com/en/facts/voices-of-huawei/statement-on-huaweis-work-with-the-african-union

Iasiello, E. (2016). China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities. Journal Of Strategic Security, Vol. 9, No. 2, 45-69.

Kennedy, A. (2019). Technology: Rapid Ascent And Global Backlash. In J.Golley, L. Jaivin, P.J. Farrelly And S.Strange (Eds.), China Story Yearbook: Power (Pp.68-85). Canberra: ANU Press.

Kharpal, A. (2021). Huawei's Growth Slowed Dramatically İn 2020 As U.S. Sanctions Take Their Toll. https://www.cnbc.com/2021/03/31/huawei-2020-revenue-growth-slows-dramatically-as-us-sanctions-hit.html

King, I., Bergen, M. and Brody, B. (2019). Top U.S. Tech Companies Begin To Cut Off Vital Huawei Supplies. https://www.bloomberg.com/news/articles/2019-05-19/google-to-end-some-huawei-business-ties-after-trump-crackdown

Kolton, M. (2017). Interpreting China's Pursuit Of Cyber Sovereignty And Its Views On Cyber Deterrence. The Cyber Defense Review, Vol. 2, No. 1, 119-154.

Lachow, I. (2011). The Stuxnet Enigma: Implications For The Future Of Cybersecurity. Georgetown Journal Of International Affairs, 118-126.

Lau, L.J. (2020). The Impacts Of The Trade War And The COVID-19 Epidemic On China-U.S. Economic Relations. China Review, Vol. 20, No. 4, 1-38.

Lee, K-F. (2018). AI Superpowers: China, Silicon Valley, And The New World Order, Boston: Houghton Mifflin Harcourt.

Lepido, D. (2019). Vodafone Found Hidden Backdoors In Huawei Equipment. https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment

Lo, C. (2019). The Sino-U.S. Tech Race: Some Myths And Realities. International Economy, Vol. 33, Issue 2, 42-45.

Lowe, J. K. (2006). Homeland Security: Operations Research İnitiatives And Applications. Interfaces, Vol. 36, No. 6, 483-485.

Mascitelli, B. Ve Chung, M. (2019). Hue And Cry Over Huawei: Cold War Tensions, Security Threats Or Anticompetitive Behaviour. Research In Globalization, Vol. 1, 1-6.

Mearsheimer, J. J. Ve Brzezinski, Z. (2005). Clash Of The Titans. Foreign Policy, Issue 146, 1-6.

Mills, J. R. (2013-14). What Ever Happened To The Front Company? Resurrecting Lost American National Security Tradecraft For An Asymmetric World. Georgetown Journal Of International Affairs, 125-133.

Mueller, M., Schmidt, A. And Kuerbis, B. (2013). Internet Security And Networked Governance İn İnternational Relations. International Studies Review, Vol. 15, No. 1, 86- 104.

Nolan, P. (2012). Is China Buying The World. Challenge, Vol. 55, No. 2, 108-118.

Phelan, D. (2019). Trump Surprises G20 With Huawei Concession: U.S. Companies Can Sell To Huawei. https://www.forbes.com/sites/davidphelan/2019/06/29/trump-surprises-g20-with-huawei-concession-u-s-companies-can-sell-to-huawei/?sh=191817801e21

Qingqing, C. ve Qiayi, L. (2020). Huawei Ban Drags China, US Into Tech Cold War. Retrieved from https://www.globaltimes.cn/content/1188623.shtml

Riikonen A. (2019). Decide, Disrupt, Destroy: Information Systems In Great Power Competition With China. Strategic Studies Quarterly, Vol. 13, No. 4, 122-145.

Shepardson, D. and Freifeld, K. (2020). Trump Extends U.S. Telecom Supply Chain Order Aimed At Huawei, ZTE. https://www.reuters.com/article/us-usa-trade-china-trump-idUSKBN22P2KG

Sherlock, T. and Bilefsky,D. (2020). Extradition of Huawei Executive Clears A Major Legal Hurdle in Canada. https://www.nytimes.com/2020/05/27/world/canada/huawei-extradition-meng-wanzhou.html

Tao, T. and Chunbu, W. (2015). The Huawei Story, California: Thousand Oaks Sage Publications.

Tarter, A. (2015). Securing Critical Infrastructure. The Military Engineer, Vol. 107, No. 697, 74-75.

Thurm, S. (2003). Huawei Admits Copying Code From Cisco in Router Software. https://www.wsj.com/articles/SB10485560675556000

Triolo, P. (2020). China's 5G Strategy: Be First Out Of The Gate And Ready To Innovate. In S. Kennedy (Ed.), China's Uneven High-tech Drive: Implications for the United States (pp.21-28). Washington: Center for Strategic and International Studies.

Tutan, U. (2019-2020). Küresel Güç Sistemlerinin Politik-Ekonomik Biçimlenişi 18. Yüzyıldan Günümüze. Briq, Cilt 1, Sayı 1, 32-44.

Tzu, S. (2000). The Art of War, Leicester: Allandale Online Publishing.

Unesco Institute for Statistics (2019). Global Investments in R&D, Fact Sheet No. 54. http://uis.unesco.org/sites/default/files/documents/fs54-global-investments-rd-2019-en.pdf

Unal, B. (2019). Cybersecurity of NATO's Space-based Strategic Assets. Chatham House Research Paper. https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf

Findings of the Invenstigation into. (2018). United States Trade Representative. https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF

Economic and trade agreement. (2020). United States Trade Representative. https://ustr.gov/sites/default/files/files/agreements/phase%20one%20agreement/Economic_And_Trade_Agreement_Between_The_United_States_And_China_Text.pdf

United States District Court For The Western District of Washington, (2017). United States Trade Representative. https://www.justice.gov/opa/press-release/file/1124996/download

Wang, B. ve He, X. (2019). What Types of Chinese ODI Activities Are Most Prone To Political Intervention. In L. Song, Y, Zhou And L. Hurst (Eds.), The Chinese Economic Transformation Views From Young Economists (Pp.263-287). Acton:ANU Press.

Wang, C. (2016). Obama's Challenge To China: The Pivot To Asia, New York: Routledge.

Waterman, S. (2011). Chinese firm 'owns' telephone system in Iraq. https://www.washingtontimes.com/news/2011/feb/21/chinese-telecom-end-ties-us-high-tech-start-/

Watts, J. (2013). NSA Accused Of Spying On Brazilian Oil Company Petrobras. https://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras

Wübbeke, J., Meissner, M., Zenglein, M. J., Ives J. And Conrad, B. (2016). Made in China 2025. Merics, No:2, 1-72.

China's Huawei helps. (2019). http://www.xinhuanet.com/english/2019-03/08/c_137876838.htm

Yuen, S. (2015). Becoming A Cyber Power: China's Cybersecurity Upgrade And Its Consequences. China Perspectives, No. 2 (102), 53-58.