Nosyon: Uluslararası Toplum ve Kültür Çalışmaları Dergisi - Nosyon: International Journal of Society and Culture Studies 2025, 15, 15-46

Bilgi, iletişim ve haberleşme teknolojileri şirketlerinin istihbarat amaçlı kullanımı: Huawei örneği[1]

Ali Kemal Özçelik[*] - Oğuz Göksu[**]

Öz

Bu çalışma, Huawei Şirketi'nin bilgi, iletişim ve haberleşme teknolojileri alanında bir istihbarat aracı olarak nasıl kullanılabileceğini incelemektedir. Huawei'nin Çin Halk Cumhuriyeti, Çin Komünist Partisi ve istihbarat-güvenlik servisleriyle olan ilişkisini analiz eden araştırma, bu bağlantının uluslararası istihbarat bağlamında doğurabileceği riskleri değerlendirmektedir. 2008-2022 yıllarını kapsayan çalışma, Huawei'nin Çin adına casusluk yaptığına dair iddiaları, şirkete yönelik yaptırımları ve güvenlik endişelerini ele almaktadır. Nitel araştırma yöntemi kullanılarak yürütülen çalışmada, elektronik gazeteler, düşünce kuruluşu raporları, mahkeme tutanakları ve akademik kaynaklardan veri toplanmış; ayrıca yarı yapılandırılmış derinlemesine görüşmelerle uzman görüşleri alınmıştır. MAXQDA Analytics Pro 2020 programı kullanılarak yapılan içerik analizleri, Huawei'nin küresel bilgi ağları üzerindeki rolünün Çin'in siber egemenlik stratejisiyle nasıl bütünleştiğini ortaya koymaktadır. Huawei'ye yönelik casusluk iddiaları, güvenlik riskleri ve bunların uluslararası yansımaları detaylı şekilde incelenmiştir. Huawei'nin telekomünikasyon altyapısında bulunan güvenlik açıkları, çeşitli ülkelerin istihbarat raporlarında potansiyel siber tehdit olarak değerlendirilmiştir. Özellikle, Huawei ekipmanlarında tespit edilen arka kapıların ulusal güvenlik riskleri oluşturabileceği belirtilmiştir. Ayrıca, Huawei'nin Çin'in Ulusal İstihbarat Yasası kapsamındaki yükümlülükleri nedeniyle Çin hükümetinin istihbarat toplama süreçlerine katkıda bulunabileceği ve bu durumun, başta ABD ve Avrupa ülkeleri olmak üzere birçok devlet tarafından uluslararası güvenlik sorunu olarak görüldüğü tespit edilmiştir Araştırma sonuçları, bilgi, iletişim ve haberleşme teknolojileri şirketlerinin istihbarat faaliyetlerinde nasıl bir karşı istihbarat sorununa dönüşebileceğini vurgulamaktadır.

Araştırma makalesi
Research article
Geliş - Submitted: 11.03.2025
Kabul - Accepted: 18.06.2025
Atıf – Reference: *Nosyon: Uluslararası Toplum ve Kültür Çalışmaları Dergisi,* 15, 15-46.

Anahtar kelimeler: Huawei, istihbarat, siber istihbarat, siber güvenlik, Çin Halk Cumhuriyeti

The intelligence utilization of information, communication, and telecommunication technology companies: The case of Huawei

Abstract

This study examines how Huawei Corporation can be utilized as an intelligence tool in the field of information, communication, and telecommunication technologies. Analyzing Huawei's relationships with the People's Republic of China, the Chinese Communist Party, and intelligence-security services, the research evaluates the potential risks this connection may pose in the context of international intelligence. Covering the period from 2008 to 2022, the study addresses allegations that Huawei engaged in espionage on behalf of China, sanctions imposed on the company, and security concerns. Conducted using qualitative research methods, the study collects data from electronic newspapers, think tank reports, court records, and academic sources; additionally, expert opinions were gathered through semi-structured in-depth interviews. Content analyses conducted using

[1] Bu çalışma; Milli Savunma Üniversitesi, Alparslan Savunma Bilimleri ve Milli Güvenlik Enstitüsü, İstihbarat Çalışmaları Anabilim Dalında yapılan "Bilgi, İletişim ve Haberleşme Teknolojileri Şirketlerinin İstihbarat Aracı Olarak Kullanılması: Huawei Şirketi Örneği" başlıklı yüksek lisans tezinden üretilmiştir.

[*] Sorumlu Yazar. Yüksek Lisans, Milli Savunma Üniversitesi, Alparslan Savunma Bilimleri Enstitüsü, İstihbarat Çalışmaları Anabilim Dalı, e-posta: ozcelikalikemal@gmail.com, ORCID-iD: 0000-0002-3072-6350

[**] Doç. Dr., Ankara Hacı Bayram Veli Üniversitesi, İletişim Fakültesi, e-posta: oguzgoxsu@gmail.com, ORCID-iD: 0000-0002-7923-8761

the MAXQDA Analytics Pro 2020 software reveal how Huawei's role in global information networks aligns with China’s cyber sovereignty strategy. Espionage allegations against Huawei, security risks, and their international implications are examined in detail. Security vulnerabilities in Huawei's telecommunications infrastructure have been identified as potential cyber threats in the intelligence reports of various countries. In particular, backdoors detected in Huawei equipment have been cited as national security risks. Furthermore, due to Huawei’s obligations under China’s National Intelligence Law, it has been found that the company could contribute to China's intelligence-gathering processes, which has been perceived as an international security issue by several states, especially the United States and European countries. The study's findings emphasize how companies in the field of information, communication, and telecommunication technologies can become counterintelligence challenges in intelligence activities.

Keywords: Huawei, intelligence, cyber intelligence, cybersecurity, People's Republic of China

Giriş

21. yüzyılda bilgi ve iletişim teknolojilerindeki hızlı gelişmeler, ulusal güvenlik stratejilerinde köklü değişiklikleri beraberinde getirmiştir. Kamu hizmetlerinin dijital ağlar aracılığıyla birbirine bağlanması, yeni güvenlik ve istihbarat paradigmalarının ortaya çıkmasına neden olmuştur. Teknolojik erişimin yaygınlaşması ve internete bağlı cihaz sayısındaki astronomik artış, siber istihbarat, siber güvenlik, endüstriyel casusluk, kritik altyapı güvenliği ve veri güvenliği gibi alanlara duyulan ilgiyi ve bu alanların güvenliğinin önemini artırmaktadır. Bu gelişmeler, yeni istihbarat kaynaklarını ortaya çıkarmış, istihbarat toplama ve analiz yöntemlerinin çeşitlenmesini sağlamıştır.

IoT Analytics verilerine göre, 2024 yılında dünya genelinde internete bağlı cihaz sayısı 18,8 milyara ulaşmıştır (IoT Analtyics, 2024). Bilginin stratejik bir unsur haline gelmesiyle, bilgi, iletişim ve haberleşme teknolojileri (BİHT) şirketleri büyük miktarda veri akışını yönetmekte, analiz etmekte ve depolamaktadır. Bu durum, devletlerin ve istihbarat topluluklarının, BİHT şirketlerini sadece ticari kuruluşlar olarak değil, aynı zamanda stratejik güvenlik aktörleri olarak değerlendirmesine yol açmıştır.

Huawei Şirketi gibi küresel çapta faaliyet gösteren BİHT şirketleri sadece teknoloji sağlayıcıları olarak değil, aynı zamanda siber güvenlik, siber istihbarat ve karşı istihbarat alanında potansiyel riskler barındıran yapılar olarak görülmektedir. 5G teknolojisinin yaygınlaşması, Huawei gibi şirketlerin küresel telekomünikasyon altyapısında oynadığı rolü daha da kritik hale getirmiştir. ABD ve müttefikleri tarafından Huawei’ye yönelik uygulanan yaptırımlar ve casusluk iddiaları, uluslararası düzeyde BİHT şirketlerinin devletlerarası güvenlik dinamikleri açısından nasıl bir risk oluşturabileceği tartışmasını gündeme getirmiştir.

Bu çalışma, Huawei örneği üzerinden bilgi ve iletişim teknolojileri şirketlerinin istihbarat faaliyetlerine nasıl dahil olabileceğini incelemektedir. Araştırmada, Çin’in siber egemenlik stratejileri, Huawei’nin organizasyonel yapısı ve uluslararası güvenlik üzerindeki etkileri ele alınmaktadır. Huawei Şirketi ve Çin Halk Cumhuriyeti’nin ulusal güvenlik ve istihbarat topluluklarıyla olan ilişkisi irdelenmektedir. Çalışma 01.01.2008 ve 31.12.2022 tarihleri arasında, Huawei Şirketi’nin Çin Devleti adına casusluk yaptığı iddia ve bulguları dikkate alması bakımından zamansal olarak sınırlandırılmıştır.

Çalışma, bilgi teknolojileri, siber istihbarat, veri/bilgi güvenliği, siber güvenlik alanlarındaki hakem niteliğindeki uzmanlarla gerçekleştirilen yarı yapılandırılmış derinlemesine görüşmelerle; Huawei Şirketi ve Çin Halk Cumhuriyeti’nin istihbarat ve güvenlik servisleri arasında var olduğu iddia edilen bağlantıları değerlendirmeyi ve bu bağlantıların istihbarat bağlamında nasıl sorunlara yol açabileceğini saptamayı amaçlamaktadır. Ayrıca, BİHT Şirketlerinin istihbarat kapasite ve yeteneklerine dair çıkarımda bulunmayı amaçlamaktadır.

Teorik çerçeve

İstihbarat kavramının birden fazla tanımının bulunması ve üzerinde uzlaşıya varılmış tek bir tanımının bulunmaması istihbarat çalışmaları alanında teorilerin geliştirilmesindeki

zorlukların temelinde yatan nedendir. Bu çalışmanın teorik çerçevesini David Kahn'ın Tarihsel İstihbarat Teorisi (*An Historical Theory of Intelligence*) oluşturmaktadır.

Kahn (Kahn, 2001, s. 91); istihbaratı 'geçmiş', 'günümüz' ve 'gelecek' başlıkları altında incelemektedir. İstihbaratın hem savaş alanında hem de ulusal güvenlik perspektifinde bugün atfedilen öneme ulaşmasında Fransız Devrimi ve Endüstri Devrimi'nin ortaya çıkardığı yeni koşulların önemli olduğunu belirtmektedir (Kahn, 2001, s. 80). İstihbarat erken dönemlerde, fiziksel nesnelerden basit yöntemlerle elde edilirken devrimlerin muhabere yöntemleri, askeri teknolojiler, teknolojiler ve toplumlar üzerindeki dönüştürücü etkisiyle birlikte istihbaratın önemi giderek artmıştır. İstihbaratın kaynakları çeşitlenmiş ve modern istihbarat olarak nitelendirilen anlayış ortaya çıkmıştır (Kahn, 2001, s. 82). Endüstri Devrimi'nin özellikle muhabere araçları üzerindeki dönüştürücü gücü, geçmişte savaşlarda dikkate alınmayan düşmanın üretim kapasitesi, ikmal hatları gibi bilgileri istihbarat için önemli kaynaklar haline getirmiştir.

Kahn, devrimlerle birlikte istihbaratın kaynaklarının çeşitlendiğini, bunların da fiziksel ve sözel istihbarat kaynakları olduğunu ifade etmektedir. Buna göre; "ilerleyen birlikler, istihkam durumları, kamp ateşleri, tank motorlarının gürültüsü" istihbaratın fiziksel kaynaklarını teşkil etmektedir (Kahn, 2001, s. 81). Geçmişte süvarilerle kısıtlı olarak toplanan fiziksel istihbarat Endüstri Devrimi ile birlikte yaşanan teknolojik gelişmelerin getirileri olan fotoğraf makineleri, casus uçaklar ve radarlar ile daha hızlı bir şekilde elde edilmeye başlamıştır.

Modern istihbaratın bugünkü önem seviyesine ulaşmasında sözel istihbaratın gelişmesinin önemli olduğu düşünülmektedir. Kahn, sözel istihbaratın örneklerini "Ele geçirilen bir askeri plan, birliklerin durumu ve motivasyonu hakkında bir rapor" olarak tanımlamaktadır (Kahn, 2001, s. 81). Devrimlerle birlikte kamuoyuna açık hükümet raporları, telgraf yazışmaları, dinlenen telsizler, üretim ve ekonomi verileri, deşifre edilen iletişim araçları, kitle iletişim araçları sözel istihbaratın önemli kaynaklarını teşkil etmektedir.

Birinci Dünya Savaşı, sözel istihbaratın daha yaygın kullanımına sahne olmuş ve bu durum istihbarata atfedilen stratejik önemin artmasına zemin hazırlamıştır. Savaşın sonuna kadar Almanya, İngiltere ve İtalya gibi önemli ülkeler askeri iletişimi deşifre edecek birimler kurmuşlardır (Kahn, 2001, s. 82). Bu durum İkinci Dünya Savaşı'nda enigma cihazının şifresinin kırılması ve savaş süresinin kısalması sonucunu ortaya çıkarmıştır.

Fransız Devrimi ve Endüstri Devrimi'nin ardından yaşanan teknolojik gelişmelerde olduğu gibi günümüzde de yaşanan teknolojik gelişmeler, istihbarat alanını dinamik olarak etkilemektedir. Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler, bürokratik ve askeri kurumları teknolojiye bağımlı hale getirmiştir. Teknoloji kullanımının demokratikleşmesi, kamu hizmetlerinin ve harekât alanının bilgi teknolojileri altyapısına bağımlı hale gelmesi güvenlik ve istihbarat alanını da şekillendirmektedir. Geçmişte telsizlerden, radyolardan, telgraflardan elde edilen sözel istihbarat günümüzde telekomünikasyon araçları, uygulamalar, alternatif medya, internete bağlı altyapılar ve siber uzaydan çeşitli yöntemlerle elde edilmektedir.

Bilgi, iletişim ve haberleşme teknolojileri şirketleri, üretmiş oldukları teknolojilerle sözel istihbaratı üreten, işleyen, depolayan önemli bir istihbarat kaynağı durumundadır. Kablolu ve kablosuz ağlar vasıtasıyla taşınan, işlenen ve depolanan veriler, istihbarat toplulukları, devletler ve şirketler için hasım aktörlerden korunması gereken sözel istihbaratın kaynaklarını teşkil etmektedir.

Huawei Şirketi'nin Çin Komünist Partisi ile olan ilişkileri, Çin Halk Cumhuriyeti'ndeki (ÇHC) istihbarat yasasının mahiyeti, şirketin Çin anakarası başta olmak üzere muhtelif coğrafyalarda bilgi teknolojileri politikalarının merkezinde olması Huawei hizmetlerinin bir karşı istihbarat sorunu oluşturabileceğine işaret etmektedir. Şirketin, bilgi, iletişim, haberleşme ve gözetim hizmetlerini kullanan ve şirket hizmetleriyle internete

bağlanan yaklaşık 4 milyar insan bulunmaktadır. Huawei Şirketi, yaklaşık 4 milyar insanın veri trafiğini yönetmekte, işlemekte ve depolamaktadır. Bu durum, şirketin aynı zamanda önemli bir sözel istihbarat kaynağı oluşturduğunu ortaya koymaktadır.

Huawei Şirketi'nin kritik altyapı sistemlerinde kullanılan ekipmanların manipüle edilmesi durumunda ortaya çıkabilecek güvenlik risklerinin boyutu şirketin önemli bir örtülü operasyon kapasitesine sahip olduğuna da işaret etmektedir.

1. İstihbarat ve bilgi iletişim ve haberleşme teknolojileri şirketleri

Bilgi, iletişim ve haberleşme teknolojilerindeki ilerlemeler, toplumsal, ekonomik, güvenlik ve bilimsel alanlarda köklü dönüşümlerin tetikleyicisi olmuştur. Küresel ölçekte ağlar üzerinden artan bağlantılılık ve bağımlılık, bireylerin günlük yaşamlarında bilgi ve iletişim teknolojilerini vazgeçilmez hale getirmiştir. Aynı şekilde, kamu hizmetlerinde gerçekleşen dijitalleşme süreci; sağlık, finans, güvenlik, ulaşım, haberleşme ve enerji altyapıları gibi kritik sektörlerin bilgi ve iletişim teknolojileri aracılığıyla yönetilmesini zorunlu kılmıştır. Bu durum, BİHT Şirketlerini istihbaratın çeşitli alanlarında önemli bir özne haline getirmektedir.

Bilgi, iletişim ve haberleşme teknolojileri ile bu alanda faaliyet gösteren şirketler, geçmişte istihbarat faaliyetlerinde araç olarak kullanılmış, günümüzde ise bu faaliyetlerin etkin ve kurumsal aktörleri haline gelmiştir. Günümüzde teknoloji kullanımının demokratikleşmesiyle birlikte BİHT kullanıcılarının sayılarındaki artış BİHT şirketlerini istihbaratın toplama, işleme ve özellikle karşı istihbarat safhaları için önemli aktörler olarak konumlanmasıyla sonuçlanmaktadır.

1.1.İstihbarat olgusu

Literatürde istihbarat olgusu/kavramı üzerinde ortak uzlaşıya varılmış bir tanımlama bulunmamaktadır. Teorisyenlere, meslek profesyonellerine, istihbarat topluluklarına ve devletlere göre zaman içerisinde değişen güvenlik ortamına uygun olarak yapılmış farklı tanımlamalar bulunmaktadır. İstihbaratı bir süreç ve nihai çıktı/ürün olarak ele alan politika belgeleri de mevcuttur.

İstihbarat faaliyetlerinde gizlilik esas olduğu için toplumlarda istihbaratın karanlık bir alan olduğuna dair algılar yerleşmiştir. Ancak, toplumlarda yerleşmiş algılardan uzak olarak istihbarat, belirli bir disiplin çerçevesinde kendi kural ve ilkelerini barındıran bir süreçtir.

Sözlük anlamlarında istihbarat, "yeni öğrenilen bilgiler, haberler, duyumlar", "zekâ, anlama ve düşünme yeteneği" ve "düşman hükümetler başta olmak üzere diğer ülkelerin hükümetleri ve/veya bu bilgileri toplayan bir grup insan" şeklinde tanımlamalar bulunmaktadır (Türk Dil Kurumu, 2025; Cambridge Dictionary, 2025). Her iki sözlükteki tanımlamalar bir araya getirildiğinde istihbarat, sistematik bir analiz sürecinden geçirilerek anlamlandırılan malumatlar bütünüdür.

Toplanan her bilgi, malumat, istihbarat niteliği taşımamaktadır. İstihbarat, yalnızca bilgilerin, malumatların toplanması safhasından oluşmamaktadır. İstihbarat ve bilgi kavramları arasında farklılıklar bulunmaktadır. Bilgi vakıf olunan her şey iken istihbarat, karar alıcıların sınırları belirlenmiş ihtiyaçlarını karşılayan bilgilerin toplandığı, analiz edildiği ve geri beslendiği analiz sürecinin bir çıktısıdır (Lowenthal, 2009, s. 9-10).

Warner (Warner, 2008), istihbaratın karar alıcılar ve meslek profesyonelleri tarafından farklı şekillerde ele alındığını ifade eder. Karar alıcılar, istihbaratı bilgi temelli bir süreç olarak kavramsallaştırırlar ve hasım aktörlere karşı avantaj sağlayacağı düşünülen her türlü veriyi bu kapsamda değerlendirirler. Meslek profesyonelleri ise istihbaratı, gizlilik prensibine dayalı ve örtülü yöntemlerin kullanıldığı bir mücadele döngüsü olarak görmektedirler. Meslek profesyonelleri istihbaratı tanımlarken istihbaratın uygulama sürecine vurgu yapmaktadırlar (Warner, 2008, s. 16). İcra edilen istihbarat faaliyetlerinin temelinde, ulusal güvenliği sağlamak, karar alma süreçlerine katkı sağlamak, uzmanlık sunmak, hasım aktörler tarafından

bilinmesi ulusal güvenlik riski ortaya çıkartacak ihtiyaç, istihbarat ve bilgilerin korunması yatmaktadır.

İstihbaratın bir diğer önemli işlevi ise stratejik sürprizlerden korunmak ve kaçınmaktadır. Stratejik sürpriz, eylemin faili ve muhatabı açısından iki şekilde tanımlanmaktadır. Fail açısından değerlendirildiğinde stratejik sürpriz; hasım aktörün güvenlik açıklarının ve zayıf yönlerinin tespit edilmesi ve "beklenmedik bir zaman diliminde, beklenmedik bir hedefe karşı kuvvet uygulanması" olarak tanımlanmaktadır (Gaddis, 2002). Eylemin muhatabı için ise hasım aktör tarafından gerçekleştirilmesine olanak tanınmayan/hesap edilmeyen eylemlerin vuku bulması durumudur.

Tarihsel süreçte savaş alanında yaşanan stratejik sürprizler, istihbarat başarısızlıkları için ders çıkarılması için önemli hadiseler olarak tanımlanmaktadır. 11 Eylül saldırısı ve Yom Kippur savaşı stratejik sürprizlerin yıkıcı sonuçlarını gösteren vakalar olarak bilinmektedir. Bu noktada, istihbaratın önemli bir işlevi stratejik sürprizlerin yaşanmasını önlemektir.

1.2. Karşı istihbarat (*Counterintelligence)*

Türkçe literatürdeki çalışmalar incelendiğinde, karşı istihbarat (counterintelligence) ve karşı casusluk (counterespionage) kavramlarının sıklıkla birbirleri yerine hatalı bir biçimde kullanıldığı görülmektedir. Kavramsal olarak karşı istihbarat faaliyetleri bir çatı olarak karşı casusluk eylemlerini de kapsamaktadır.

Karşı istihbarat, yabancı istihbarat topluluklarının operasyonlarını önlemek, bozmak ve aldatma amacıyla icra edilen faaliyetlerdir. İstihbarat topluluklarının veya istihbarat müşterilerinin güvenliklerine yönelik hasım istihbarat toplulukları tarafından gerçekleştirilebilecek her türden düşmanca istihbarat faaliyetini tespit etme ve karşı koyma sürecidir (Prunckun, 2019, s. 27). Karşı istihbarat kapsamı bakımından karşı casusluğa göre çok daha geniş aktörlerle ilgilenmektedir. Ulusal güvenliği tehdit edebilecek yabancı istihbarat toplulukları, devletler, devlet dışı aktörler, bireyler ve terörizm unsurları gibi aktörlerin tamamına karşı yürütülen bir süreçtir.

Karşı casusluk, aktif karşı istihbarat faaliyetleri içerisinde değerlendirilmektedir. Hedef olarak yalnızca yabancı istihbarat toplulukları bulunmaktadır (Stelee, 2007, s. 3). Karşı casusluk faaliyetlerin temelinde; hedef olarak belirlenen yabancı istihbarat topluluğu personelleriyle temas geliştirme, personelleri devşirme, yanıltma, yönlendirme ve kurumu manipüle etme amaçlanır. Hedef istihbarat topluluğunun iç işleyişine dair gizli bilgilere erişmeyi ve operasyonlarını arzu edilen doğrultuda yönlendirmek amaçlanır.

Karşı istihbarat, eylem türlerine göre savunma amaçlı (defensive) ve taarruzi (offensive) olmak üzere ikiye ayrılmaktadır (Prunckun,2019, s. 28). Savunma Amaçlı Karşı İstihbarat (SAKİ), istihbarat topluluğu içerisindeki güvenlik açıklarını veya zayıflıkları tespit ederek hasım aktörlerin bu zafiyetleri istismar etmelerini önleme, düşmanca eylemleri tespit ederek caydırmayı amaçlayan faaliyetler bütünüdür. SAKİ, "tespit" ve "caydırıcılık" ilkelerinin etkili bir biçimde uygulanmasına dayanır (Prunckun, 2008, s. 55). Caydırıcılık, hasmane aktörlerin yürütmekte olduğu veya planladığı istihbarat faaliyetlerinden vazgeçmesini sağlamayı hedefler. Bu strateji, karşı tarafın gerçekleştireceği eylemin ciddi ve telafi edilemez sonuçlar doğuracağı mesajını ileterek tehdit oluşturan unsurları engellemeye dayanır. Tespit süreci ise güvenlik ihlallerini belirlemek, şüpheli kişiler arasındaki örgütsel bağları analiz etmek ve ilgili delilleri toplamaktan oluşur (Prunckun, 2008, s. 55-56). Örneğin, gizli bir belgenin sızdırılması durumunda, belgede erişim yetkisi bulunan kişilerin incelenmesi ve bağlantılarının araştırılması ve akabinde tespit edilen kişi/kişilerin motivasyonlarının belirlenmesi gerekmektedir.

Karşı istihbarat sürecinin temelini dört soru oluşturmaktadır; "(i) Neyi korumak istiyoruz? (ii) Rakiplerimiz hakkımızda ne öğrenmek istiyor?, (iii) Hangi yöntemle öğrenmeye çalışıyor?, (iv) Gizli bilgilerimizi korumak için hangi yöntem ve taktikleri

kullanabiliriz?" (Bernhardt, 2003 s. 33). SAKİ'nin öncelikleri dışarıdan içeriye yönelebilecek tehditlere karşı sistematik önlemler almaktır. Mekânsal güvenlik, personel güvenliği, bilgi güvenliği iletişim ve haberleşme güvenliği hepsi bir bütünün ayrılmaz parçalarıdır.

Taarruzi Karşı İsthbarat (TKİ), 'tespit', 'aldatma' ve 'etkisiz hale getirme' ilkelerini içeren agresif bir süreçtir. Amaç, hasım aktörün karşı istihbarat süreçlerinde hangi teknik ve yöntemleri kullandığını algılama, hedef istihbarat topluluğu içerisinde çift taraflı olarak çalışabilecek elemanları tespit etme, tehditleri etkisiz hale getirme ve hasım aktörün eylemlerini manipüle etme süreçlerini kapsamaktadır (Zegart, 2022, s. 152). TKİ eylemlerinin başarılı olmasının ön koşulu SAKİ gerekliliklerinin sağlanmış olmasına bağlıdır.

Aldatma ilkesi, hedef aktörün gerçeklik algısını manipüle ederek kararlarını yönlendirmeyi amaçlar. Whaley (2020), aldatmayı "yanlış veya çarpıtılmış bir gerçeklik algısını kabul ettirmeye yönelik manipülasyon süreci" olarak tanımlarken, Clark (2019, s. 11), bunu "hedefin gerçeklik algısına avantaj sağlayacak şekilde yanlış bilgi empoze etme süreci" olarak açıklamaktadır. Aldatma operasyonları, hedef aktörün düşünce yapısını şekillendirerek rakip karşısında stratejik avantaj elde etmeye dayanır.

Etkisizleştirme, düşman istihbarat toplulukları veya hasım aktörlerin yürütmekte olduğu ya da planladığı istihbarat operasyonlarını bertaraf etmeyi hedefler. Bu süreçte, ulusal güvenlik açısından korunması gereken kişi, kurum, bilgi ve altyapılara yönelik tehditlerin ortadan kaldırılması esastır. Prunckun'a (2017, s. 216) göre, etkisizleştirme, iki temel yöntemle gerçekleştirilebilir:

- Felç (Paralysis): Hasım aktörelerin operasyonlarının geçici olarak sekteye uğratılması.
- Yıkım (Disruption): Casus hücrelerinin açığa çıkarılması, tutuklanması veya şüpheli personelin kritik bilgiye erişiminin kısıtlanması.

Bu yöntemlerin amacı, hedef aktörün güven kaybı yaşamasına ve yürüttüğü operasyonlara olan ilgisini kaybetmesine neden olmaktır.

21.yüzyılda teknolojinin hızla gelişmesi, TKİ ve SAKİ uygulamalarının siber istihbarat ve siber tehdit istihbaratı alanlarına yönelmesine neden olmuştur. Günümüzde devletler ve istihbarat teşkilatları, geleneksel yöntemlerin yanı sıra siber alanda da karşı istihbarat faaliyetlerini güçlendirmektedirler. Kritik altyapıların korunması, bilgi güvenliği ve mahremiyeti, siber altyapının bir bütün olarak siber uzayı da kapsayacak şekilde güçlendirilmesine yönelik hem savunmacı hem de saldırgan stratejiler geliştirmektedir.

1.3.Tarihte bilgi, iletişim ve haberleşme teknolojileri şirketleri ve istihbarat ilişkisi

BİHT şirketleri, ticari faaliyetler yürüten kuruluşlar olmanın ötesinde, devletler ve istihbarat servisleri için stratejik birer araç haline gelmiştir. Özellikle büyük ölçekli teknoloji şirketleri, devletlerin istihbarat toplama, gözetim, örtülü operasyon ve siber operasyonlarını desteklemek amacıyla kullanılabilmektedir. Tarihte birçok örnek, BİHT şirketlerinin istihbarat servisleriyle yakın ilişkiler içinde olduğunu ve örtülü operasyonlara dahil edildiğini göstermektedir. Bu bağlamda, Rubicon Operasyonu, Pegasus Yazılımı ve Cambridge Analytica Skandalı, devletlerin ve istihbarat servislerinin BİHT şirketleriyle ilişkisini gözler önüne seren önemli vakalardır.

Rubicon Operasyonu, Soğuk Savaş döneminde Amerikan Merkezi İstihbarat Teşkilatı (CIA) ve Alman Dış İstihbarat Servisi (BND) tarafından yürütülen örtülü bir istihbarat operasyonudur. Operasyon, İsviçre merkezli Crypto AG adlı şirketin satın alınarak istihbarat faaliyetleri için kullanılması yoluyla gerçekleştirilmiştir. Crypto AG, 1950'lerden itibaren dünya çapında devletlere şifreleme cihazları satan bir şirket olarak bilinmektedir. Ancak, 1970'lerin başında CIA ve BND tarafından gizlice satın alınarak şirketin ürettiği ekipmanlar "arka kapı" erişimleriyle manipüle edilmiştir (Miller & Warrell, 2020, s. 42). Böylece, Crypto AG'nin ürettiği şifreleme cihazlarını kullanan yaklaşık 120 ülke ve uluslararası kuruluşun gizlilik derecesine sahip belgeleri ve iletişim trafikleri CIA ve BND istihbarat servisleri

tarafından takip edilebilmiştir (Fagel, 2020, s. 67). Bu vaka, teknoloji şirketlerinin istihbarat servisleri tarafından manipüle edilerek küresel gözetim mekanizmalarına entegre edilebileceğini göstermektedir.

Bir başka örnek vaka ise İsrail merkezli NSO Group tarafından geliştirilen Pegasus isimli casus yazılımdır. Yazılım, hedef kişilerin cep telefonlarına bulaşarak sesli ve yazılı iletişimlerini izleyebilme, kamera ve mikrofonlarını kullanabilme, anlık konum verilerini takip edebilme gibi özelliklere sahiptir (Marczak vd., 2021, s. 23). Pegasus'un en dikkat çeken özelliği, "zero-click" (tıklama gerektirmeyen) saldırı yöntemleriyle çalışmasıdır. Yani, hedef kişinin herhangi bir bağlantıya tıklamasına veya dosya indirmesine gerek kalmadan, yazılım telefona sızabilmektedir (Scott-Railton vd., 2021, s. 45). Bu durum, istihbarat servislerine hedef bireyleri gizlice takip etme ve iletişimlerini ele geçirme imkânı sağlamaktadır.

2021 yılında sızdırılan Pegasus Project raporuna göre, Pegasus yazılımı Fransa Cumhurbaşkanı Emmanuel Macron, Pakistan Başbakanı İmran Han, Fas Kralı VI. Muhammed ve Yunanistan muhalefet lideri Nikos Androulakis gibi üst düzey devlet yetkililerini hedef almak için kullanılmıştır (Amnesty International, 2021, s. 78). Ayrıca, gazeteciler, aktivistler ve insan hakları savunucuları gibi birçok sivil hedef de Pegasus yazılımı aracılığıyla gözetlenmiştir.

Bir diğer önemli vaka ise Cambridge Analytica skandalıdır. Cambridge Analytica skandalı BİHT şirketlerinin psikolojik operasyonlarda nasıl kullanılabileceğini gösteren önemli vakalardan birisidir. 2018 yılında ortaya çıkan skandal, Cambridge Analytica adlı veri analiz şirketinin Facebook kullanıcılarının verilerini izinsiz bir şekilde topladığı ve demokratik tercihleri yönlendirmek için kullandığını ortaya koymuştur (Cadwalladr, 2019, s. 29).

Şirket, 2016 ABD Başkanlık Seçimleri ve Brexit Referandumu dahil olmak üzere birçok demokratik süreçte mikro-hedefleme yöntemiyle seçmen davranışlarını etkilemeye çalıştığı tespit edilmiştir. Hedefli olarak belirlenen 50 milyon kullanıcının kişisel verilerini işleyerek psikografik profilleri çıkarılmış ve hedeflenmiş siyasi reklamlar sunularak seçmen tercihleri yönlendirmek amaçlanmıştır (Kogan & Kosinski, 2018, s. 51). Bu vaka, BİHT şirketlerinin büyük veri işleme yoluyla psikolojik operasyonlar için nasıl kullanılabileceğini ve demokratik süreçleri nasıl manipüle edebileceğini gözler önüne sermektedir (Zuboff, 2019, s. 210). Cambridge Analytica skandalı, istihbarat servisleri ve büyük teknoloji şirketleri arasındaki ilişkinin sadece geleneksel casusluk ve gözetimle sınırlı olmadığını, aynı zamanda örtülü kamuoyu operasyonlarında da etkili olarak kullanılabileceğine işaret etmektedir.

Huawei ve benzeri telekomünikasyon şirketlerinin de benzer şekilde devlet destekli istihbarat operasyonlarına dahil edilip edilmediği, uluslararası güvenlik camiasında tartışmalı bir konu olmaya devam etmektedir (Inkster, 2019, s. 154).

2. Çin Halk Cumhuriyeti'nin siber egemenlik politikaları ve Huawei

Siber egemenlik, devletlerin kendi dijital altyapıları, internet erişimi, veri yönetimi ve siber güvenlik politikaları üzerinde tam denetim sağlama yetisi olarak tanımlanmaktadır (Deibert, 2019, s. 45). Siber egemenlik kavramı, devletlerin dijital bağımsızlıklarını koruma ve yabancı ülkelerden gelen siber tehditlere karşı önlem alma gerekliliği çerçevesinde ortaya çıkmıştır. Geleneksel egemenlik anlayışı sınır güvenliği, askeri güç ve diplomasiye dayalıyken, siber egemenlik çağdaş uluslararası sistemde veri akışı, dijital altyapı ve siber güvenlik politikalarının kontrol edilmesi anlamına gelmektedir (Segal, 2020, s. 113).

Siber egemenlik kavramı, ilk olarak 2010 yılında ÇHC Devlet Konseyi Bilgi Ofisi tarafından yayımlanan "Çin'de İnternet" başlıklı beyaz kitapta kullanılmıştır (Information Office of the State Council of the People's Republic of China, 2010). ÇHC, siber uzayı ulusal

egemenliğin önemli bir bileşeni olarak görmekte ve devletin interneti kendi politik, kültürel ve hukuki çerçevesi içinde yönetme hakkına sahip olduğunu savunmaktadır.

Çin'in bu yaklaşımı, 2012 yılında Budapeşte Siber Konular Konferansı'nda uluslararası alana taşınmıştır. Konferansta yapılan açıklamada "Her ülke, kendi tarihsel, kültürel ve hukuki gelenekleri çerçevesinde interneti yönetme hakkına sahiptir" ifadelerine yer verilmiştir (Statement at Budapest Conference on Cyber Issues, 2012).

Çin, yıllar içinde siber egemenlik anlayışını geliştirmiş ve bu normu uluslararası alanda kabul ettirme çabalarını sürdürmüştür. 2014 yılında Wuzhen Deklarasyonu ile kavram daha da genişletilmiş ve "Ülkeler, interneti kullanma ve yönetişim haklarına saygı göstermeli, başka devletlerin siber egemenliğini ihlal edecek faaliyetlerden kaçınmalıdır" ifadesiyle vurgulanmıştır. 2016 yılında yayımlanan "Ulusal Siber Uzay Stratejisi" belgesinde ise devletlerin siber uzayda düzeni koruma ve ulusal güvenliği tehdit eden zararlı içerikleri önleme hakkına sahip olduğu belirtilmiştir (China's National Cyberspace Strategy, 2016).

Çin'in siber egemenlik yaklaşımı, Batılı ülkelerin "siber açıklık" ve "siber özgürlük" ilkelerine karşıt bir politika izlemekte olup, internetin devlet denetiminde olması gerektiği anlayışına dayanmaktadır. Çin Komünist Partisi (ÇKP)bu normun benimsenmesi ile hem ulusal hem de uluslararası alanda bir dizi stratejik hedefi gerçekleştirmeyi amaçlamaktadır (Karmazin, 2023, s. 63):

- Rejim istikrarını sağlamak ve ÇKP'nin otoritesini güçlendirmek amacıyla, bilgi akışı üzerinde tam kontrol sağlanarak dijital ortamda muhalif seslerin önlenmesi hedeflenmektedir.
- Eğitim, medya ve ekonomi gibi devlet kontrolündeki sektörlerde internet teknolojilerinin yaygınlaştırılması, böylece ÇKP'nin ideolojik denetiminin dijital ortamda da sürdürülmesi sağlanmaktadır.
- Kritik altyapı ağlarının güvenliğinin artırılması yoluyla, siber saldırılar ve kötü niyetli dijital operasyonlara karşı ulusal güvenliğin korunması amaçlanmaktadır.
- Yabancı teknolojiye bağımlılığı azaltmak ve Çin'in teknolojik özerkliğini sağlamak için hukuki düzenlemeler ve ekonomik teşvikler uygulanmaktadır.
- Siber uzay stratejileri kapsamında ABD ve Batılı ülkelerin dijital alandaki etkisini sınırlamak, Çin'in küresel rekabetteki konumunu güçlendirmek için temel bir hedef olarak benimsenmektedir.

ÇHC siber egemenlik kavramını bir devlet politikası olarak ele almaktadır. Bu doğrultuda yasal düzenlemeler, ekonomik teşvik ve yatırımlar ve teknoloji girişimlerini hayata geçiren ülkelerin başında gelmektedir (Triolo & Webster, 2017, s. 16). Çin, siber egemenliğini sağlamak amacıyla "Made in China 2025" programı ve "Dijital İpek Yolu" gibi projeleri hayata geçirerek teknoloji üretimini ve küresel ağ üzerindeki etkisini artırmayı hedeflemektedir.

Çin'in teknoloji politikalarının temel taşlarından biri "Made in China 2025" (MIC2025) programıdır. Çin Devlet Konseyi tarafından 2015 yılında duyurulan bu stratejik plan, Çin'in küresel teknoloji lideri olmasını ve kritik endüstrilerde dışa bağımlılığını azaltmasını hedeflemektedir (Kennedy, 2018, s. 4). MIC2025 programı kapsamında yarı iletkenler, telekomünikasyon, yapay zekâ ve siber güvenlik teknolojileri öncelikli alanlar olarak belirlenmiştir.

MIC2025 programının temel öncelikli 10 hedefi sırasıyla şunlardır (PRC State Council, 2015):

i) "Yeni nesil bilgi teknolojisi endüstrisi,
ii) Gelişmiş CNC makineleri ve robotlar,
iii) Havacılık ve Uzay teçhizatı
iv) Deniz mühendisliği ekipmanları ve yüksek teknolojili gemiler
v) Gelişmiş demiryolu ulaşım ekipmanı
vi) Enerji tasarrufu ve yeni enerji araçları

vii) Güç(elektrikli) ekipmanları
viii) Tarım makine ve ekipmanları
ix) Yeni malzemeler
x) Biyoteknoloji, ilaç ve tıbbi cihazlar."

Bu program kapsamında Huawei, ZTE, Alibaba ve Tencent gibi büyük Çinli teknoloji firmaları ulusal güvenlik ve dijital egemenlik projelerinde önemli roller üstlenmiştir (Lee, 2020, s. 58). MIC2025'in telekomünikasyon ve dijital altyapı bileşeninde Huawei, Çin hükümeti tarafından desteklenen ve teşvik edilen en önemli aktörlerden biri olarak öne çıkmaktadır (Kania, 2019, s. 34).

Özellikle 5G teknolojisinin geliştirilmesi MIC2025'in en kritik bileşenlerinden biri olarak değerlendirilmektedir. Huawei, 5G altyapısını geliştirerek Çin'in küresel siber egemenlik stratejisinde temel bir rol oynamaktadır. MIC2025 programının uzun vadeli hedefi, Huawei gibi firmaların küresel teknoloji pazarındaki etkisini artırarak Çin'in siber egemenliğini güçlendirmektir.

Çin'in siber egemenlik politikalarının bir diğer önemli ayağı "Dijital İpek Yolu" (Digital Silk Road) projesidir. Dijital İpek Yolu, Çin'in Kuşak ve Yol Girişimi (KYG) kapsamında dijital altyapı, 5G ağları, veri merkezleri, fiber optik kablo projeleri ve yapay zekâ teknolojileri üzerine yoğunlaşan küresel bir stratejidir (Hillman & Sacks, 2021, s. 87).

Dijital İpek Yolu Projesinin temel hedefleri şu şekilde özetlenebilir (Triolo vd., 2020, s. 45):

- Çin'in küresel internet altyapısını inşa ederek dijital ticaret ağlarını genişletmek,
- Çinli teknoloji firmalarının (Huawei, ZTE, Alibaba, Tencent) küresel pazarda lider konuma gelmesini sağlamak,
- Çin'in dijital ekonomi üzerinden etkisini artırarak, gelişmekte olan ülkelerde teknoloji bağımlılığı yaratmak,
- Çinli firmaların küresel telekomünikasyon projelerinde baskın aktör haline gelmesini sağlamak.

Huawei, Dijital İpek Yolu Projesi kapsamında Asya, Afrika, Latin Amerika ve Orta Doğu'daki ülkelere dijital altyapı ve 5G teknolojileri sağlamaktadır. Özellikle Afrika kıtasında Huawei'nin kurduğu fiber optik ağlar ve 5G altyapıları, Çin'in bölgedeki dijital etkisini artırmaktadır (Feldstein, 2019, s. 63). Huawei'nin projede üstlendiği misyon, yalnızca telekomünikasyon altyapısı kurmakla sınırlı değildir. Şirket, Çin hükümeti tarafından desteklenen projelerde akıllı şehir teknolojileri, yüz tanıma sistemleri, büyük veri analitiği ve siber güvenlik çözümleri de sağlamaktadır. Özellikle "Güvenli Şehir Projeleri" adı altında Huawei, Çin'in siber gözetim modelini ihraç etmektedir. Uganda, Zambiya ve Pakistan gibi ülkelerde Huawei destekli akıllı şehir sistemleri, hükümetlerin dijital gözetim yeteneklerini artırarak halk üzerindeki denetimlerini güçlendirmesine olanak tanımaktadır (Feldstein, 2020, s. 78).

Uluslararası güvenlik perspektifinde, Huawei'nin küresel ölçekte siber istihbarat toplama ve işleme noktasındaki potansiyeli Çin devletine stratejik veri sağlayabileceği endişesini ortaya çıkarmaktadır (Segal, 2020, s. 127). Bu sebeple, ABD, Avrupa Birliği ve bazı müttefik ülkeler, Huawei'nin 5G altyapısına erişimini kısıtlama ve alternatif tedarik zincirleri oluşturma yönünde çeşitli adımlar atmıştır (Kaska vd., 2019, s. 88).

2.1.Ulusal istihbarat yasası

Çin, BİHT şirketlerini yalnızca ulusal düzeyde değil, küresel ölçekte de siber egemenlik stratejisinin bir parçası olarak konumlandırmaktadır. AR-GE yatırımları, kamu-özel-akademi iş birlikleri, hibe finansman ve uluslararası yatırımlar yoluyla desteklenen bu şirketler, Çin devletinin dijital alandaki nüfuzunu artırmada kritik bir rol üstlenmektedir. Ayrıca, yürürlüğe konulan yasal düzenlemeler, gerekli görülen durumlarda bu şirketlerin Çin'in ulusal güvenlik

ve istihbarat çıkarlarına hizmet etmesini zorunlu kılmaktadır. Bu bağlamda, Çin'in Ulusal İstihbarat Yasası'nın 7. Maddesi Çin'in siber egemenlik politikalarıyla ilişkilendirilmekte ve bununla birlikte, mezkûr yasanın Çin menşeli şirketler üzerinde bağlayıcılığı olacağına dair tartışmalar devam etmektedir.

ÇHC'nin kamuoyuna açıklanan ilk resmi istihbarat yasası olan "Ulusal İstihbarat Yasası" 2017 yılında Ulusal Halk Daimî Komitesi tarafından onaylanmış ve 27 Haziran 2017 tarihinde yürürlüğe girmiştir. Bu yasa, Batılı ülkelerdeki istihbarat yasalarından farklı olarak spesifik istihbarat teşkilatlarına doğrudan atıfta bulunmamakta, bunun yerine devlet güvenlik organları, kamu güvenlik organları ve askeri istihbarat teşkilatlarını "milli istihbarat teşkilatları" olarak tanımlamaktadır. Bu belirsizlik, Çin'in istihbarat yapılanmasının muğlak bir çerçevede şekillendiğini ve sivil-askeri bütünleşik bir yapı izlediğini göstermektedir (National Intelligence Law, 2017).

Ulusal İstihbarat Yasası'nı uluslararası alanda tartışmalı hale getiren kuşkusuz yasanın muğlaklığı ve dolayısıyla 7. maddenin sınırlarının belirlenmemiş olmasıdır. Çin Ulusal İstihbarat Yasası'nın 7. maddesine göre (National Intelligence Law, 2017); "Tüm kuruluşlar ve vatandaşlar, ulusal istihbarat çabalarını yasalara uygun olarak destekleyecek, yardım edecek ve iş birliği yapacak ve farkında oldukları ulusal istihbarat çalışma sırlarını koruyacaklardır. Devlet, ulusal istihbarat çabalarını destekleyen, yardım eden ve iş birliği yapan kişi ve kuruluşları korur." Buradaki muğlak tanıma göre; İstihbarat faaliyetlerinin yürütülmesinde bir seferberlik anlayışı bulunmaktadır. Ülkede faaliyet gösteren kurum, kuruluş ve vatandaşlar istihbarat faaliyetlerini desteklemekle yükümlüdür.

Özellikle yasa metininde yer alan "tüm kuruluşlar" ifadesi, Huawei ve diğer Çinli BİHT şirketlerinin, faaliyet gösterdikleri ülkelerde Çin hükümetinin istihbarat taleplerini karşılamakla yükümlü olduğuna işaret etmektedir. Bu zorunluluk, kullanıcıları aracılığıyla veri toplama, depolama ve işleme kabiliyetlerine sahip olan BİHT şirketlerini önemli bir karşı istihbarat sorunu haline getirmektedir. İlgili yasa maddesinin son kısmında yer alan "*Devlet, ulusal istihbarat çabalarını destekleyen, yardım eden ve iş birliği yapan kişi ve kuruluşları korur"* ibaresi ise bir ödül-ceza sistemine atıfta bulunmaktadır. Çin'in siber egemenlik politikasının önemli araçlarından olan BİHT şirketleri, ÇHC'nin taleplerini karşıladığı müddetçe ÇKP mekanizmasının sağladığı ayrıcalıklardan yararlanabilecek olduğu şeklinde yorumlanabilir. Çin'in Ulusal İstihbarat Yasası'nın mezkûr maddeleri devlet-şirket iş birliğini kurumsallaştırarak, Çin'in uluslararası istihbarat kapasitesini artırmasına olanak tanımaktadır.

2.2. Huawei Şirketi ve Çin Halk Cumhuriyeti devleti arasındaki ilişki

a) Huawei şirketinin kuruluşu

ÇKP, ülke ekonomisini büyütmek, telekomünikasyon altyapısını güçlendirmek ve yabancı teknolojiye olan bağımlılığı azaltmak amacıyla 1986 yılında kapsamlı bir telekomünikasyon altyapısını iyileştirme planı oluşturmuştur. Bu strateji, Çin'in yerli teknoloji geliştirme hedefleri doğrultusunda belirlenen üç temel ilkeden oluşmaktadır (Wen, 2017, s. 66): "(i) Doğrudan ekipman ithalatı, (ii) teknolojik aktarım ve özümseme, (iii) Çinli şirketlerin çok uluslu teknoloji devlerini yakalama ümidi ile yerli inovasyon".

Bu strateji doğrultusunda Huawei, Çin hükümetinin teknoloji ve altyapı hedeflerine uygun olarak 1987 yılında Ren Zhengfei tarafından Shenzhen'de kurulmuştur. Shenzhen, Çin'in özel ekonomik bölgelerinden biri olup, sağladığı vergi avantajları, yatırım teşvikleri ve esnek işgücü politikalarıyla Huawei'nin hızlı büyümesine olanak sağlamıştır (Wen, 2017, s. 66). Huawei'nin kurucusu Ren Zhengfei, Çin Halk Kurtuluş Ordusu'nun (PLA) Bilgi Teknolojileri Araştırma Birimi'nde askeri teknoloji uzmanı olarak görev yapmıştır. Bu durum, Huawei'nin Çin devletiyle bağlantılı olup olmadığına dair çeşitli tartışmaları beraberinde getirmiştir. Batılı ülkeler, Huawei'nin Çin hükümetinin doğrudan desteğiyle

hareket eden bir şirket olduğunu ve ulusal güvenlik açısından potansiyel bir tehdit oluşturduğunu öne sürmektedir.

Kuruluş yıllarında telefon anahtarları (phone switches) üretimiyle faaliyet gösteren Huawei, zamanla mobil geniş bant cihazları, telekomünikasyon ağları, giyilebilir teknoloji ve akıllı cihazlar alanlarında büyüyerek küresel bir teknoloji devi haline gelmiştir. Şirketin resmî belgelerinde misyonu ve vizyonu, "tamamen bağlantılı ve akıllı bir dünya inşa etmek" olarak tanımlanmaktadır. Huawei, bu hedef doğrultusunda 5G teknolojisi, yapay zekâ, akıllı lojistik sistemleri ve mobil geniş bant cihazları alanlarında yaptığı yatırımlarla sektörün en önemli aktörlerinden biri haline gelmiştir (Huawei, 2021).

Şirket, Ar-Ge yatırımlarına büyük önem vermekte olup 2016 yılı itibariyle yıllık gelirinin %10'undan fazlasını Ar-Ge çalışmalarına ayırmaktadır. Huawei bünyesinde çalışanların yaklaşık %50'si Ar-Ge projelerinde görev almakta olup, şirketin dünya çapında beş araştırma laboratuvarı ve 40.000 farklı kategoride 100.000'den fazla aktif patenti bulunmaktadır (Huawei, 2020). Huawei, Asya'dan Avrupa'ya, Avrupa'dan Afrika'ya kadar geniş bir coğrafyada telekomünikasyon altyapısı sağlayan lider şirketlerden biri olarak konumlanmıştır. 2021 yılı verilerine göre Huawei, 55.4 milyar dolarlık marka değeriyle altyapı hizmetleri sağlayan şirketler arasında en yüksek değere sahip şirketlerden biri olmuştur (Alsop, 2023).

Huawei'nin küresel teknoloji sektöründeki konumu, Çin'in ulusal teknoloji politikalarıyla doğrudan ilişkili olup, şirketin devlet sübvansiyonları ile hızlı yükselişi ve rekabet gücü uluslararası alanda çeşitli tartışmalara neden olmaktadır. Huawei Şirketi'nin iddia edildiği gibi bir özel şirket olmadığı, bir kamu-özel iştiraki olduğu üzerine tartışmalar devam etmektedir.

b) Şirketin finansmanı

Huawei Şirketi'nin bir kamu-özel ortaklığı olduğuna dair iddiaların temelinde ve Huawei'nin kısa süre içerisinde küresel bir başarıya ulaşmasında şirketin kamu bankalarından aldığı sübvansiyonlar ve idari yapısı yatmaktadır. Bu kapsamda şirketin kamu bankalarından aldığı hibe ve kredilerin incelenmesi önemlidir. Huawei'nin küresel ölçekteki başarısında birçok faktör etkili olmakla birlikte, ucuz işgücü, geniş iç pazar ve devlet destekli finansman mekanizmaları, Huawei'nin dünya çapında telekomünikasyon sektöründe lider konuma yükselmesine katkıda bulunmuştur. Çin devlet bankalarının sağladığı finansman desteği, vergi indirimleri ve teşvikler, Huawei'nin rekabet gücünü artırmış ve özellikle gelişmekte olan ülkelerdeki pazar payını genişletmesine olanak tanımıştır.

Her ne kadar Huawei yöneticileri şirketin devlet desteği almadığını ifade etse de, Shenzhen Belediyesi ÇKP Sekreteri Li Youwei'nin (Hou, 2019) ifadelerine göre, Huawei'nin ilk mali desteği 1990 yılında Shenzhen Construction Bank tarafından sağlanan 30 milyon Yuan tutarındaki düşük faizli kredi ile gerçekleşmiştir. Bu tür finansman destekleri, Huawei'nin başlangıç aşamasında sermaye ihtiyacını karşılamasına ve Ar-Ge faaliyetlerine yatırım yapmasına olanak sağlamıştır.

Huawei, Çin hükümetinin yerli teknoloji üretimini teşvik eden politikaları kapsamında desteklenen şirketlerden biri olarak, 1996 yılında yürürlüğe giren "Çin Halk Cumhuriyeti Bilimsel ve Teknolojik Kazanımların Dönüşümünü Teşvik Kanunu" ile vergi muafiyetleri, düşük faizli krediler ve doğrudan hibe desteği gibi avantajlardan yararlanmıştır. Bu teşviklerin temel amacı, yerli şirketleri uluslararası pazarda güçlendirmek ve yabancı teknoloji firmalarının Çin pazarındaki etkisini azaltmaktır (Gilley, 2000, s. 94-96).

Huawei ve ZTE gibi diğer büyük telekomünikasyon şirketleri, Çin hükümetinin yüksek teknoloji geliştirme alanındaki kapasitesini artırma hedefiyle başlattığı 863 ve 973 programları kapsamında önemli finansal destekler almıştır. Bu destekler, Ar-Ge yatırımlarını

artırarak küresel rekabette avantaj sağlamak amacıyla oluşturulmuştur (U.S.-China Economic and Security Review Commission, 2011, s. 61).

Huawei'nin Çin devlet bankalarından sağladığı büyük çaplı finansmanlar şirketin büyümesine önemli katkılar sağlamıştır. Bu finansman destekleri arasında, 1998 yılında China Construction Bank'tan 3,9 milyar Yuan, 1999'da Industrial and Commercial Bank of China (ICBC) ve Bank of China'dan 3,5 milyar Yuan, Ar-Ge yatırımları için ICBC'den 200 milyon Yuan, 2004 yılında China Development Bank'tan 10 milyar dolar, Ex-Im Bank of China'dan sağlanan 630 milyon dolarlık düşük faizli kredi bulunmaktadır (Gilley, 2000, s. 94-96).

Huawei, devlet desteğiyle yalnızca iç pazarda değil, aynı zamanda uluslararası projelerde de genişleme stratejileri uygulamış ve Çin hükümeti tarafından "Ulusal Şampiyon" olarak sınıflandırılmıştır. Bu kapsamda Huawei, ZTE, China Telecom ve Bank of China gibi büyük ölçekli devlet destekli kuruluşlarla birlikte kamu-özel iş birliği çerçevesinde küresel projelere dahil edilmiştir (U.S.-China Economic and Security Review Commission, 2011, s. 61).

Çin devlet bankalarının Huawei'ye sağladığı destek iki temel yöntemle gerçekleşmektedir. İlk yöntem, doğrudan finansman desteği sağlanarak Huawei'nin Ar-Ge ve üretim yatırımlarına sermaye aktarımı ve ikinci yöntem, Huawei ile ticari ilişkiler geliştirecek uluslararası müşterilere sağlanan yüksek tutarlı krediler ile şirketin küresel pazarda avantaj elde etmesini sağlamak.

Bu yöntemlerden ikincisi, Huawei'nin özellikle gelişmekte olan ülkelerdeki pazarlara girişini kolaylaştıran enstrümanlardan biri olarak değerlendirilmektedir. Çin devlet bankalarının sunduğu finansman destekleri, Huawei ürünlerini kullanmayı taahhüt eden yabancı hükümetlere yönelik kredi anlaşmalarını içermektedir. Bu strateji, bazı çevreler tarafından "borç tuzağı diplomasisi" olarak nitelendirilmekte ve Çin'in küresel ekonomik etkisini artırma stratejilerinden biri olarak değerlendirilmektedir.

Bu tür anlaşmalara bir örnek olarak, 2017 yılında Burundi hükümetinin, telekomünikasyon altyapısını modernize etmek amacıyla Huawei ile 30 milyon dolarlık bir anlaşma imzalaması gösterilebilir. Bu projenin finansmanı, Huawei International Co. Limited tarafından sağlanan 30 milyon dolarlık kredi ile gerçekleştirilmiştir (GlobalComms Database, 2017).

Benzer şekilde, Huawei, Avrupa ve Rusya pazarında da Çin devlet bankalarının sağladığı yüksek tutarlı krediler aracılığıyla varlığını genişletmiştir. 2007 yılında Polonya'nın en büyük 3G operatörlerinden biri olan Play'e, China Development Bank tarafından Huawei ekipmanlarının satın alınması şartıyla 640 milyon Euro tutarında kredi tahsis edilmiştir (Tucker, Anderlini & Parker, 2008). 2009 yılında Rusya merkezli mobil operatör MegaFon, China Development Bank'tan Huawei ekipmanlarının satın alınması koşuluyla 300 milyon dolarlık bir kredi almıştır (Reuters, 2009).

Bu tür finansman mekanizmaları, Huawei'nin sadece Çin iç pazarında değil, küresel ölçekte genişlemesine ve rekabet avantajı elde etmesine yardımcı olmuştur. Ancak, Huawei'nin Çin devlet bankaları aracılığıyla sağlanan finansmanlarla genişlemesi, şirketin bir kamu-özel iştiraki olduğu iddialarını güçlendirmektedir.

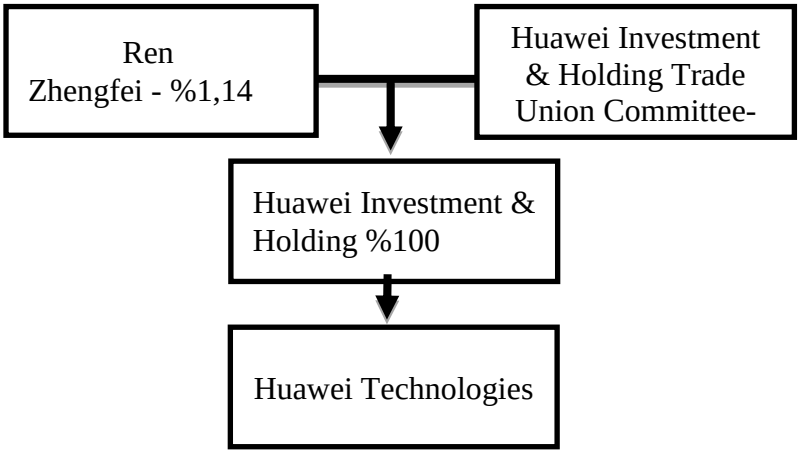
c) Şirketin idari yapısı

Huawei, çeşitli iştirakleri ve bağlı kuruluşları bünyesinde barındıran bir holding yapısına sahip olup, şirketin ana faaliyetlerini Huawei Technologies Inc. ve Huawei Investment & Holding Co. yürütmektedir. Huawei Technologies Inc., Huawei Investment & Holding Co.'nun tamamen sahip olduğu bir iştiraktir (Huawei, 2022).

Huawei'nin idari yapısı ve hissedarlık modeli, uzun yıllardır akademik ve uluslararası çevrelerde tartışma konusu olmuştur. Şirketin resmî açıklamalarına göre, Huawei'nin büyük hissedarı ve sahibi, şirket çalışanlarıdır. Huawei, hisselerinin "Çalışan Hisse Senedi Sahipliği

Programı" (Employee Stock Ownership Program, ESOP) kapsamında şirket çalışanlarına ait olduğunu ve üçüncü tarafların şirket üzerinde doğrudan bir tasarrufu bulunmadığını iddia etmektedir (Huawei, 2022).

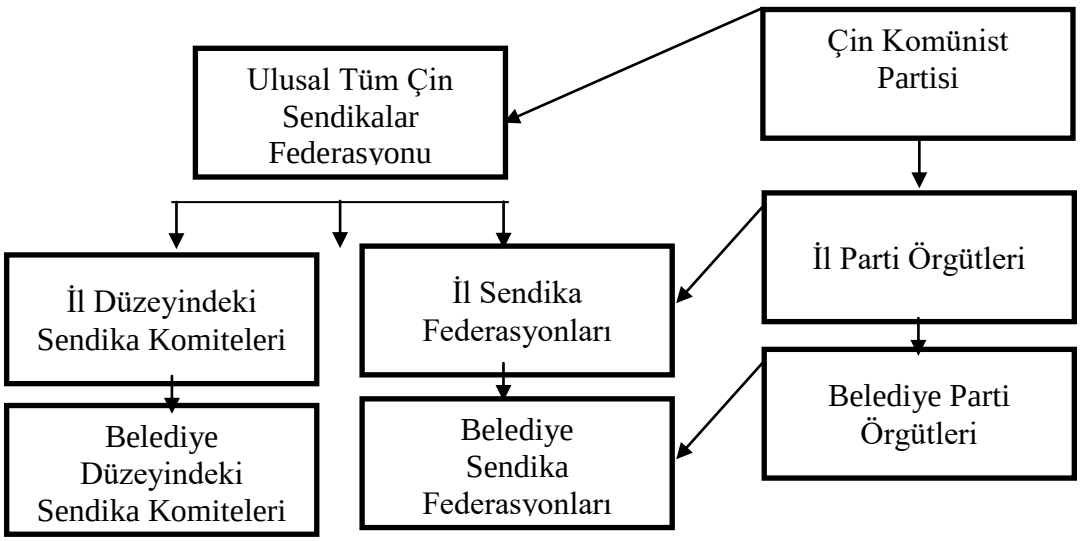
2021 yılı itibarıyla Huawei Technologies bünyesinde 195 binden fazla çalışan bulunmaktadır ve şirketin tek hissedarı Huawei Investment & Holding Co. olarak görünmektedir (Huawei, 2022). Ancak, şirketin kurucusu Ren Zhengfei'nin hisselerin yalnızca %1,14'üne sahip olduğu, geri kalan %98,86'lık hissenin Huawei Investment & Holding Company Trade Union Committee adlı bir sendika bünyesinde toplandığı ifade edilmektedir (Balding & Clarke, 2019, s. 8).

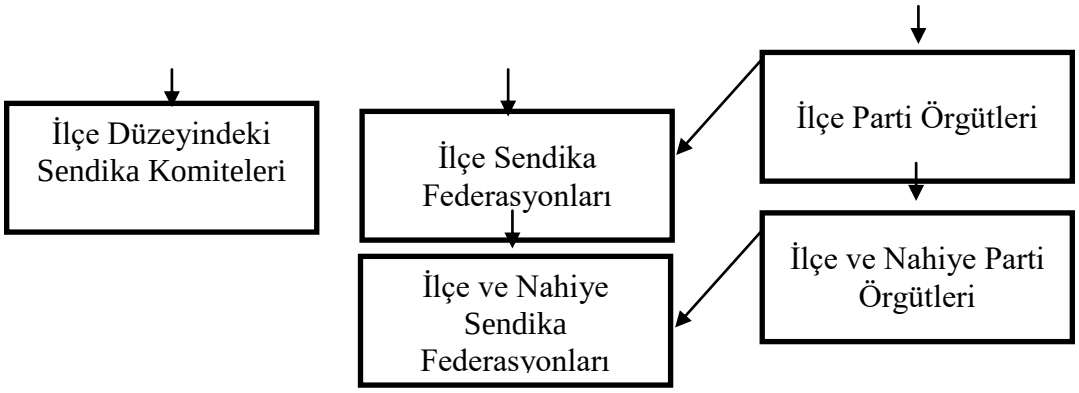


Şekil 1. Huawei şirketinin hisse dağılımı (Balding, 2019, s. 8)

Huawei çalışanlarının sahip olduğu hisseler adi hisselerden farklıdır ve "sanal hisse" (virtual shares) olarak tanımlanmaktadır. Bu sistem kapsamında, çalışanlar kâr payı elde edebilirken, hisselerini devretme ya da üçüncü bir tarafa satma hakkına sahip değildir (Yang, 2019).

Huawei Investment & Holding Company bünyesinde bulunan hisseler, ÇHC'nin sendikalarla ilgili yasal düzenlemelerine tabi olup, ÇKP tarafından denetlenen Tüm Çin Sendikalar Federasyonu (All-China Federation of Trade Unions, ACFTU) çatısı altında yönetilmektedir (The President of PRC, 2009). Çin'de tüm sendikalar devlet kontrolü altında faaliyet göstermekte ve doğrudan ÇKP tarafından yönetilmektedir (China Daily, 2018). Bu bağlamda, Huawei çalışanlarının hisse sahipliğinin bağımsız olmadığı ve sendika aracılığıyla şirketin dolaylı olarak Çin hükümeti ve ÇKP kontrolü altında olduğuna işaret etmektedir. Sendikanın yönetim yetkisinin tamamen ÇKP tarafından belirlendiği göz önüne alındığında, Huawei'nin gerçekten bağımsız bir özel şirket olup olmadığı tartışmalı hale gelmektedir.





Şekil 2. Tüm Çin Sendikalar Federasyonu'nun ÇKP ile ilişkisi (Estlund, 2017, s. 49)

Huawei'nin yönetim yapısını ele alan tartışmaların temelinde, şirketin gerçek sahipliğinin belirsizliği yatmaktadır. ÇHC Şirketler Hukuku'nun 24. Maddesine göre, bir limited şirketin en fazla 50 hissedarı olabilir (The President of PRC, 2009). Bu sınırlama nedeniyle, Huawei'nin hisseleri yasal olarak tek bir hissedar tarafından temsil edilmekte ve sendika bünyesinde toplanmaktadır. Ancak, Huawei'nin çalışanlarının hisse sahipliği hakkında kamuoyuna sunduğu bilgiler, şirketin gerçek sahipliğini doğrulamak açısından yetersizdir (Balding & Clarke, 2019, s. 8).

Özellikle, Huawei'nin sahiplik yapısının sendikalar aracılığıyla düzenlenmesi ve sendikaların ÇKP tarafından denetlenmesi, şirketin bağımsızlığına dair ciddi soru işaretleri yaratmaktadır. Tüm Çin Sendikalar Federasyonu'nun başkanı Wang Dongming'in aynı zamanda Ulusal Halk Kongresi Daimi Komitesi Başkan Yardımcılığı görevini yürütüyor olması, federasyonun doğrudan ÇKP kontrolü altında olduğunu göstermektedir (China Daily, 2018). Bu durum, Huawei'nin sadece özel bir şirket olmadığı, aksine Çin devleti ve ÇKP tarafından yönetilen bir stratejik aktör olduğunu kanıtlar niteliktedir.

2.3.Şirkete yönelik yargı süreci ve yaptırımlar

Batılı hükümetler ve güvenlik kurumları, Çin menşeli teknoloji şirketlerinin küresel ölçekte artan etkisini ulusal güvenlik açısından bir tehdit olarak değerlendirmektedir. Çin'in siber casusluk, ekonomik casusluk ve etki operasyonları konusundaki geçmişi, bu endişelerin temelini oluşturmaktadır. 2013 yılında Mandiant tarafından yayımlanan APT1 raporu, Çin Halk Kurtuluş Ordusu (HKO) ile bağlantılı olduğu tespit edilen bir hacker grubunun, 140'tan fazla kuruluşun hassas verilerini hedef aldığını ortaya koymuştur. ABD Adalet Bakanlığı verilerine göre, 2011-2018 yılları arasında tespit edilen ekonomik casusluk vakalarının %90'ı Çin ile ilişkilendirilmektedir (Demers, 2018).

Çin menşeli şirketlere yönelik güvenlik endişelerinin bir diğer temel nedeni ise Çin'in yasal düzenlemeleri ve şirketlerin devletle zorunlu iş birliği yükümlülüğüdür. 2014 yılında yürürlüğe giren Karşı İstihbarat Yasası ve 2017 Ulusal İstihbarat Yasası, şirketleri ve bireyleri istihbarat faaliyetlerine destek vermekle yükümlü kılmaktadır. Bu durum, Huawei ve benzeri şirketlerin Çin hükümeti adına istihbarat toplama faaliyetlerine katkıda bulunabileceği iddialarını güçlendirmektedir. Ayrıca, bazı Huawei projelerinde tespit edilen güvenlik açıkları da bu endişeleri pekiştirmektedir (Demers, 2018).

Arka kapılar, bir sistemin güvenlik protokollerini aşarak yetkisiz erişime olanak sağlayan güvenlik açıklarıdır. Bu açıklar, kötü amaçlı yazılımlar aracılığıyla oluşturulabileceği gibi, sistem geliştiricileri tarafından bilinçli olarak da sisteme entegre edilebilir (Thomas & Francillon, 2018). Donanım tabanlı arka kapılar, üretim sürecinde cihazlara eklenebildiği gibi, saldırganlar tarafından cihaz veya ağ bileşenlerinde yapılan değişikliklerle de oluşturulabilir (Kim vd., 2010).

Huawei'ye yönelik arka kapı iddiaları, uluslararası kamuoyunda dikkat çeken tartışmalardan biri olmuştur. Vodafone, Huawei'nin 2009-2011 yılları arasında İtalya'da sağladığı telekomünikasyon altyapılarında arka kapılar tespit ettiğini açıklamıştır. Huawei, bu açıkların sistemsel hatalardan kaynaklandığını ve giderildiğini belirtmişse de operatör şirketin talebine rağmen güvenlik açıklarının tamamen ortadan kaldırılmadığı tespit edilmiştir (Lepido, 2019).

ABD Ulusal Güvenlik Danışmanı Robert O'Brien, Huawei'nin dünya genelinde sattığı sistemlerde hassas ve kişisel verilere gizlice erişebildiğine dair kanıtlar bulunduğunu iddia etmiştir. Ancak, bu kanıtlar yalnızca Alman istihbarat servisleriyle paylaşılmış ve kamuoyuna açıklanmamıştır (Pancevski, 2020).

Huawei cihazlarının potansiyel olarak kullanıcı verilerine yetkisiz erişim sağladığı iddialarına dair bazı vakalar da bulunmaktadır. Kasım 2022'de Çin'deki koronavirüs protestolarında Huawei marka telefonlarla çekilen bazı videoların cihazlardan otomatik olarak silindiği iddia edilmiştir. Çinli sosyal medya kullanıcıları, Huawei telefonlarının hükümetin baskıcı önlemlerine yönelik protestoları kaydetmelerini engellemek amacıyla manipüle edilmiş olabileceğini öne sürmüştür (France 24, 2022).

Huawei'nin Çin hükümetiyle olan ilişkisi, yalnızca siber casusluk ve güvenlik açıklarıyla sınırlı kalmamaktadır. Şirket, Çin'de yürütülen geniş çaplı gözetim projelerine de entegre edilmiştir. Özellikle, Uygur Türkleri ve diğer etnik azınlıkların takip edilmesi için geliştirilen gözetim sistemlerinde Huawei'nin rol oynadığı iddia edilmektedir.

ÇHC Kamu Güvenliği Endüstri Standartları'nda, Uygur Türkleri'ni Han kökenli vatandaşlardan ayırabilecek yüz tanıma sistemlerine atıfta bulunulmaktadır (Çin Halk Cumhuriyeti Kamu Güvenliği Endüstri Standartları, 2017). Huawei ve Megvii, 2018 yılında Çin Devlet Fikri Mülkiyet Ofisi'ne, bu teknolojiyle bağlantılı bir patent başvurusunda bulunmuştur. Bu durum, Huawei'nin Çin hükümetinin gözetim ve kontrol mekanizmalarıyla doğrudan iş birliği içinde olduğuna dair önemli bir göstergedir (Çin Halk Cumhuriyeti Devlet Fikri Mülkiyet Ofisi, 2018).

2011 yılında ABD hükümeti, Huawei şirketine yönelik ilk resmi soruşturmayı başlatmıştır. Bu süreç, ABD Meclisi Daimî Seçilmiş İstihbarat Komitesi tarafından yürütülmüş olup, soruşturmanın temel amacı, Çin merkezli Huawei Technologies Co. Ltd. ve ZTE Corporation'ın ABD'deki telekomünikasyon ve kritik altyapı sektörlerinde oluşturabileceği güvenlik ve karşı istihbarat risklerini belirlemek olmuştur (The House Permanent Select Committee on Intelligence, 2012).

ABD Adalet Bakanlığı, 2019'da Huawei'ye yönelik bir iddianame hazırlamış, şirketin İran yaptırımlarını ihlal ettiği ve ABD'li teknoloji firmalarına karşı endüstriyel casusluk yaptığı iddia edilmiştir. Soruşturma, Huawei'ye yönelik güvenlik kaygılarının 2007'ye dayandığını göstermiştir. Huawei'nin İran'daki yan kuruluşu Skycom Tech Co. Ltd.'nin yaptırımlara uymadığı şüphesiyle başlatılan incelemede, Temmuz 2007'de ifadesi alınan ve "Birey-1" olarak kodlanan kişinin, Huawei'nin kurucusu Ren Zhengfei olduğu ve ABD yetkililerini kasıtlı olarak yanılttığı tespit edilmiştir (United States District Court Eastern District of New York, 2019).

İddianame sürecinde elde edilen bulgular üzerine Pentagon, Çin'in askeri gözetleme yapabileceği şüphesiyle askeri üslerde Huawei ve ZTE telefon satışını kısıtlamıştır. Ardından, devlet kurumlarının Huawei ve ZTE ekipmanları almasını ve sözleşme yapmasını yasaklayan Ulusal Savunma Yetki Yasası yürürlüğe girmiştir. Bu yasa, Huawei'ye ek olarak Hytera, Hikvision, Dahua ve bağlı şirketlerin kamu kuruluşlarında kullanımını da kısıtlamaktadır (Mccain, 2018, s. 283).

Bu bulgular ve yaptırımlar, Huawei'nin yalnızca telekomünikasyon altyapısı sağlayan bir şirket olmadığı, aynı zamanda Çin hükümetinin güvenlik ve istihbarat faaliyetlerine dolaylı veya doğrudan katkı sağladığına işaret etmektedir.

3. Bilgi, iletişim ve haberleşme teknolojileri şirketlerinin istihbarat aracı olarak kullanılması: Huawei Şirketi üzerinden bir araştırma

3.1 Araştırma modeli

Bu araştırmada, olayları anlamak, açıklamak ve yorumlamak amacıyla nitel araştırma yöntemi kullanılmıştır. Nitel araştırma, belirli bir durumu veya olguyu derinlemesine incelemek, farkındalık kazanmak ve karmaşık ilişkileri ortaya çıkarmak için tercih edilen bir yöntemdir. Nitel araştırmalar, gözlem, görüşme ve doküman analizi gibi veri toplama tekniklerini kullanarak, olayları doğal ortamlarında bütüncül bir şekilde ele almayı amaçlar (Yıldırım & Şimşek, 2021, s. 37).

Bu çalışmada nitel araştırma türlerinden görüşme yöntemi kullanılmış ve araştırma deseni olarak fenomenolojik yaklaşım benimsenmiştir. Fenomenoloji, bireylerin yaşadıkları deneyimlere odaklanarak, belirli bir olgunun nasıl algılandığını ve anlamlandırıldığını incelemeyi amaçlayan bir yaklaşımdır.

3.2. Evren örneklem

Nitel araştırmalarda sıkça kullanılan amaçlı örnekleme yöntemleri, araştırmanın derinlemesine analizine katkı sağlayan önemli bir metottur. Bu yöntem, araştırma konusu ile ilgili değerli bilgilere sahip olduğu düşünülen bireylerin belirlenmesini ve incelenmesini sağlamaktadır. Amaçlı örnekleme, özellikle belirli olgu ve olayların keşfedilmesi ve açıklanması açısından büyük önem taşımaktadır (Yıldırım & Şimşek, 2021, s. 116).

Araştırmanın örneklemi amaçlı örnekleme yöntemi kullanılarak belirlenmiş ve 12 kişiden oluşmuştur. Çalışma grubunun, konunun farklı boyutlarını yansıtacak şekilde farklı sektörlerden uzmanları içermesine özen gösterilmiştir. Bu doğrultuda, dört kamu personeli, üç akademisyen ve beş özel sektör çalışanı örnekleme dahil edilmiştir. Bu çeşitlilik, maksimum çeşitlilik örnekleme stratejisine dayanmaktadır. Maksimum çeşitlilik örnekleme, farklı meslek gruplarının bakış açılarını ortaya koyarak, araştırma konusunun farklı yönlerini belirginleştirmeyi amaçlar. Burada genelleme yapma amacı güdülmemekte, aksine, örneklemi oluşturan bireylerin deneyimlerinin ortak veya farklı yönlerinin analiz edilmesi hedeflenmektedir (Yıldırım & Şimşek, 2021, s. 117-118).

Araştırmada örneklem seçimi için belirli kriterler oluşturulmuştur:

Meslek	Unvan	Çalışma deneyimi	Ülke
Kamu personeli 1	Daire başkanı	22 yıl	Türkiye
Kamu personeli 2	Mühendis	5 yıl	Türkiye
Kamu personeli 3	Mühendis	7 yıl	Türkiye
Kamu personeli 4	Araştırmacı	4 yıl	Türkiye
Akademisyen 1	Prof. Dr.	18 yıl	ABD
Akademisyen 2	Doç. Dr.	9 yıl	Polonya
Akademisyen 3	Dr. Ögr. Üyesi	5 yıl	Türkiye
Özel sektör 1	Yönetici (manager)	14 yıl	Türkiye
Özel sektör 2	Orta düzey (mid)	4 yıl	Türkiye
Özel sektör 3	Kıdemli (senior)	8 yıl	ABD
Özel sektör 4	Kıdemli (senior)	10 yıl	Türkiye
Özel sektör 5	Kıdemli (senior)	7 yıl	Almanya

Tablo 1. Çalışmaya katılan hakem niteliğindeki uzmanlar hakkında bilgiler

3.3. Veri toplama aracı

Bu araştırmada veri toplama yöntemi olarak yarı yapılandırılmış görüşme formu kullanılmıştır. Yarı yapılandırılmış görüşmeler, önceden belirlenmiş ancak esneklik sağlayan açık uçlu sorular içeren bir yöntemdir. Bu yaklaşım, araştırmacının belirlenen sorulara bağlı kalarak ek sorular yöneltmesine ve konuyu derinlemesine irdelemesine imkân tanımaktadır (Yıldırım & Şimşek, 2021, s. 130).

Araştırmada, kamu personeli, akademisyenler ve özel sektör çalışanları olmak üzere farklı sektörlerde faaliyet gösteren uzmanlarla yüz yüze, çevrimiçi platformlar ve elektronik posta yoluyla görüşmeler gerçekleştirilmiştir. Görüşmeler sırasında belirlenen sorulara bağlı kalınmakla birlikte, katılımcıların yanıtlarına göre esneklik sağlanmıştır.

Görüşme formunun hazırlanma sürecinde bir danışma kurulu oluşturulmuş ve kurulda görüşme yöntemi üzerine akademik çalışmaları bulunan bir akademisyen, bilgi güvenliği alanında çalışan bir kamu personeli ve özel sektörde beş yıl deneyimi olan bir siber güvenlik uzmanı yer almıştır. Danışma kurulunun değerlendirmeleri doğrultusunda sorular revize edilerek araştırma amacına uygun hale getirilmiştir.

Veri toplama sürecinde karşılaşılan zorluklar arasında, özellikle kamu personeliyle gerçekleştirilen görüşmelerde gizlilik hassasiyeti nedeniyle ses kaydı alınamaması yer almaktadır. Bu durum, görüşme sürelerinin uzamasına ve verilerin yazılı olarak not alınarak kaydedilmesine neden olmuştur. Benzer şekilde, çevrimiçi platformlarda gerçekleştirilen bazı görüşmelerde de katılımcılar ses kaydına rıza göstermemiştir.

Çalışma kapsamında, Huawei Şirketi'nin çeşitli ülkelerdeki yöneticileriyle iletişim kurularak şirkete söz hakkı tanınmak istenmiştir. Ancak, şirket yöneticileri çeşitli çekincelerin öne sürerek veya iletişim çabalarını yanıtsız bırakarak çalışmaya katılmamışlardır.

Görüşmelere ek olarak, ABD Ulusal İstihbarat Daimi Komitesi'nin Huawei Şirketi hakkında yürüttüğü soruşturmanın mahkeme tutanakları, 2021 yılında Huawei Şirketi hakkında yayınlanan ABD Kongresi raporu da titizlikle incelenmiştir. Bununla birlikte; düşünce kuruluşları olan Hoover Instituon'ın "On strategic surprise", Citizen Lab'ın "NSO Group's Pegasus spyware: A technical analysis", Mandiant'ın APT1 raporu ve CSIS'in "China's Digital Silk Road: Implications for global technology competition." başlıklı raporlarından faydalanılmıştır. Bunlara ek olarak; çalışmanın güncelliğini koruması bakımından The Guardian, The Wall Street Journal, France 24 ve Bloomberg elektronik gazetelerinin konu ile ilgili haberlerinden faydalanılarak çalışmanın kaynakları çeşitlendirilmiştir.

3.4. Verilerin analizi

Araştırmada yarı yapılandırılmış görüşmelerden elde edilen veriler, içerik analizi tekniği ile incelenmiştir. Bu teknik, verilerin sistematik olarak analiz edilerek sınıflandırılmasını, benzer verilerin kavramlar ve temalar etrafında bir araya getirilerek yorumlanmasını amaçlamaktadır (Yıldırım & Şimşek, 2021, s. 250).

Araştırma kapsamında 12 katılımcının verdiği yanıtlar MAXQDA Analytics Pro 2020 (Release 20.4.0) paket programı aracılığıyla analiz edilmiştir. Analiz süreci şu adımlardan oluşmaktadır:

- Katılımcıların yanıtları MAXQDA'nın belge sistemine eklenmiş,
- Tüm yanıtlar satır satır kodlanarak işlenmiş,
- Benzer kodlar bir araya getirilerek alt temalar ve temalar oluşturulmuş,
- Sonuç olarak 11 tema ve beş alt tema belirlenmiştir.

Bulguların daha net sunulabilmesi için MAXMaps kullanılarak çeşitli grafik ve şekiller oluşturulmuş, ayrıca kod-matris tarayıcı ile elde edilen verilerin katılımcılara göre dağılımı belirlenmiştir. Şekil 3 kodlama süreçlerine ilişkin genel bir özet sunmaktadır.

Kod Sistemi	KP.1	KP.2	KP.3	KP.4	ÖS.1	ÖS.2	ÖS.3	ÖS.4	ÖS.5	PR.1	PR.2	PR.3	TOP...
Kontrol ve gözetim	1	2	2	1	3	3	1	2	1	2	3	2	23
Savaş ve barış dönemi	4	3	2	4	5	4	2	2	2	4	4	3	39
Yabancı teknolojiye bağımlılık ve güvenli	4	2	2	1	3	3	1	1	1	2	4	2	26
Güvenlik açıkları													0
Açıklar	1	1	2	1	2	1	3	1	1	4	2	1	20
Bilinçli açıklar	3	3	1	1	1	3	5	1	2	3	2	4	29
İstihbarat faaliyetlerinin desteklenmesi	2	2	1	1	1	3	3	1	2	3	1	2	22
5G teknolojisi ve üretici	1	1	1	1	1	2	5	1	2	4	2	1	22
Tedarikçi seçiminde parametreler	5	4	3	2	3	3	5	6	3	4	5	4	47
Huawei Şirketi ve Çin Halk Cumhuriyeti	3	2	2	1	1	2	3	1	2	2	3	2	24
Huawei Şirketi													0
Paylaşma zorunluluğu olan veriler	1	2	2	1	2	2	2	2	2	1	2	2	21
Veri mahremiyeti ve güvenlik	1	1	1	1	1	1	1	2	1	1	1	1	13
Potansiyel riskli teknolojileri	1	2	1	1	1	4	2	1	2	3	2	2	22
Huawei ekipmanları ve ulusal güvenlik	3	2	2	2	1	1	1	1	3	1	2	2	21
Uluslararası tartışmaların temel unsurları	1	2	1	1	1	3	3	2	1	2	2	1	20
TOPLAM	31	29	23	19	26	35	37	24	25	36	35	29	349

Şekil 3. Temalar, alt temalar ve katılımcılar

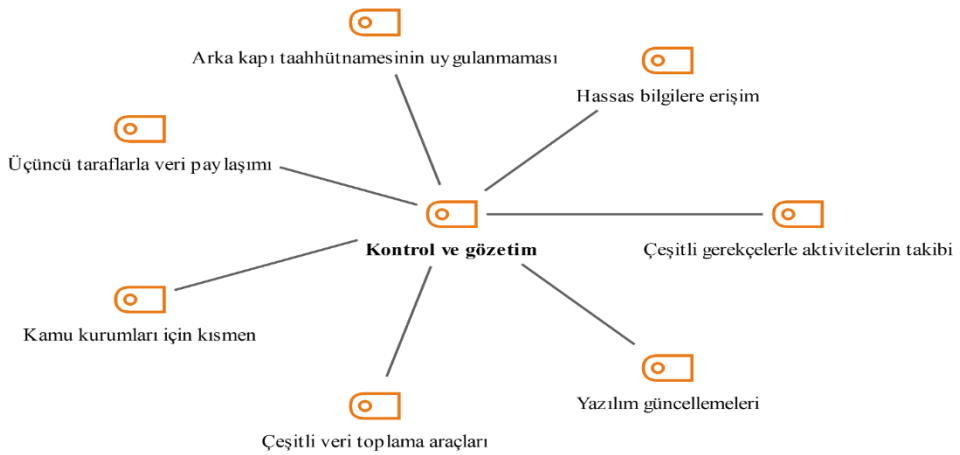
3.6. Araştırmanın bulguları

Araştırmanın bulguları, içerik analizi yöntemiyle elde edilen temalar, alt temalar, kategoriler ve kodlar doğrultusunda sistematik bir şekilde sunulmaktadır. Bu süreçte, elde edilen veriler belirli başlıklar altında sınıflandırılmış, benzer içerikler bir araya getirilerek anlamlı bir bütün oluşturulmuştur. Bulgular, katılımcıların doğrudan ifadeleriyle desteklenmiş, görüşlerin içeriği korunarak analiz edilmiştir.

Ayrıca, analiz edilen verilerin daha iyi anlaşılmasını sağlamak amacıyla temaların dağılımı, alt temaların ilişkileri ve kodlamaların detayları çeşitli şekiller, tablolar ve görselleştirme araçları kullanılarak açıklanmıştır. Bu sunum yöntemi, araştırmanın güvenilirliğini ve tutarlılığını artırmayı hedeflemekte olup, katılımcı ifadelerinin özgünlüğünü ve çeşitliliğini yansıtacak şekilde düzenlenmiştir.

(i) Kontrol ve gözetim

Katılımcılar, bilgi, iletişim ve haberleşme teknolojileri şirketlerinin, son kullanıcıya yönelik teknolojik ekipmanlar üzerindeki kontrol ve gözetim kapasitesini değerlendirmiştir. Bu değerlendirmeye ilişkin katılımcı görüşleri, Şekil 4 ve Tablo 2'de ayrıntılı olarak sunulmuştur.



Şekil 4. Kontrol ve gözetim temasının kodları

Kodlar	Frekans	Katılımcılar
Çeşitli gerekçelerle aktivitelerin takibi	6	ÖS.1, ÖS.2, ÖS.3, ÖS.4, PR.2, PR.3
Çeşitli veri toplama araçları	5	KP.2, ÖS.1, ÖS.5, PR.1, PR.2
Yazılım güncellemeleri	5	KP.2, ÖS.2, PR.1, PR.2, PR.3
Kamu kurumları için kısmen	3	KP.3, KP.4, ÖS.1
Üçüncü taraflarla veri paylaşımı	2	ÖS.2, ÖS.4
Hassas bilgilere erişim	1	KP.3
Arka kapı taahhütnamesinin uygulanmaması	1	KP.1

Tablo 2. "Kontrol ve gözetim" temasının kodları, frekansları ve katılımcıları

Katılımcılar, bilgi, iletişim ve haberleşme teknolojileri şirketlerinin, son kullanıcı cihazları üzerindeki kontrol ve gözetim kapasitesine ilişkin farklı değerlendirmelerde bulunmuştur. Üç katılımcı, özellikle kamu kurumlarında kapalı devre sistemlerin kullanılması nedeniyle kontrol ve gözetimin kısmen mümkün olabileceğini ifade etmiştir. Altı katılımcı, uzaktan destek ve teknik sorunların çözümü gibi gerekçelerle kullanıcı aktivitelerinin takip edildiğini, bunun da zorunlu kullanıcı sözleşmeleri aracılığıyla dayatıldığını belirtmiştir. Beş katılımcı, yazılım güncellemeleri gibi işlemlerle cihazlar üzerinde kısıtlı kontrol sağlayan şirketlerin, konum bilgileri ve tüketici alışkanlıkları gibi verileri topladığını vurgulamıştır. İki katılımcı, elde edilen verilerin ticari ya da ulusal güvenlik gerekçeleriyle üçüncü taraflarla paylaşılabileceğini ifade etmiştir. Ayrıca, bir katılımcı, konum verileri ve hassas bilgilerin erişilebilir olduğunu, bir diğer katılımcı ise arka kapı taahhütnamesine uyulmadığını ve bunun şirketlere hizmetler üzerinde geniş bir kontrol ve gözetim kapasitesi sağladığını ileri sürmüştür.

> **KP.3.:** "Kısmen kontrol ve gözetip kapasitesine sahiptir. Benim de çalıştığım bazı kamu kurumları kapalı devre sistem ile çalışmaktadır. Burada veri trafik yoğunluğu denetlemelerimizle herhangi bir akış, yoğunluk var mı tespit edebiliyor. Bu sistemlere dışarıdan müdahale güçtür. Öyle ki bazı sistem güncellemelerini dahi manuel olarak yaparız."

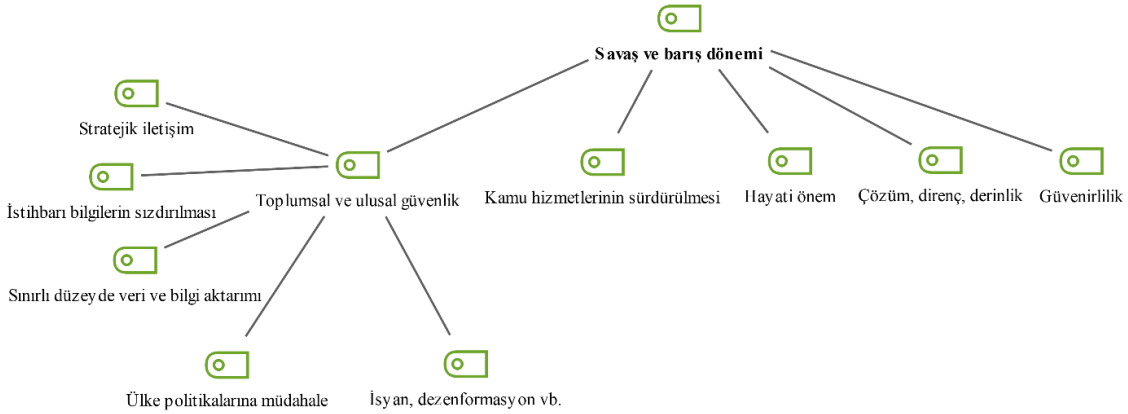
> **ÖS.2.:** "Şirketlerin güvenlik açıklarını kapatmak, yeni özellikler eklemek ve performansı arttırmak amacıyla işletim sistemi üzerinde gerçekleştirdiği yazılım güncellemeleri mevcuttur. Bu her ne kadar kullanıcı memnuniyeti için yapılıyor olsa da aynı zamanda bu şirketlere cihazlar üzerinde uzaktan kontrol yetkisi de vermektedir. Kullanıcı verileri kimi zaman ticari amaçlarla kimi zaman ulusal güvenlik gerekçeleriyle üçüncü taraflarla paylaşılır. İstihbarat boyutuyla düşünüldüğünde; Şirketlerin sınırsız gözetim kapasitesi ve verileri de mahiyetine göre istihbarat süreci için uygun kaynaklar olarak yorumlarsak sınırsız toplama kapasitesi bulunmaktadır."

> **PR.1.:** "Bilgi, iletişim ve haberleşme teknolojileri şirketleri, son kullanıcı tarafından kullanılan teknolojik ekipmanlar üzerinde gözetim kapasitesine sahiptir. Bu şirketler, yazılım güncellemeleri, hizmet şartları, gizlilik politikaları ve kullanıcı etkileşimlerini izleme yoluyla kullanıcı davranışları üzerinde etkili bir denetim sağlayabilir. Ayrıca, cihazlara önceden yüklenmiş uygulamalar veya işletim sistemleri aracılığıyla da kullanıcı verilerine erişim elde edebilirler. Bu durum, kullanıcıların mahremiyeti ve veri güvenliği konusunda önemli soruları beraberinde getirir."

> **KP.1:** "Taahhütnamelerin içerisinde hizmet sağlayıcı ekipman ve hizmetlerinde arka kapı (Backdoors) bulunmayacağına dair taahhüt verir. Ancak, bu taahhüttün aksine birçok yazılım ve ekipman içerisinde art niyetli veya bilinçsiz olarak arka kapılar barındırmaktadır. Bu noktada bilgi, iletişim ve haberleşme teknolojileri şirketlerinin nihai çıktıları olan hizmetleri üzerinde kontrol ve gözetim kapasitesine sahiptir."

(ii) Savaş ve barış dönemlerinde bilgi, iletişim ve haberleşme teknolojileri şirketlerinin önemi

Katılımcılar, savaş ve barış dönemlerinde altyapı hizmeti sağlanan bilgi, iletişim ve haberleşme teknolojileri şirketlerinin stratejik önemi hakkında görüşlerini ifade etmişlerdir. Bu değerlendirmeler Şekil 5 ve Tablo 3'te detaylı olarak sunulmuştur.



Şekil 5. "Savaş ve barış dönemi" temasının kodları

Kodlar	Alt kodlar	Frekans	Katılımcılar
Kamu hizmetlerinin sürdürülmesi		9	KP.1, KP.2, KP.3, KP.4, ÖS.1, ÖS.4, ÖS.5, PR.1, PR.3
Hayati önem		8	KP.3, KP.4, ÖS.3, ÖS.4, ÖS.5, PR1, PR.2. PR.3
Çözüm, direnç, derinlik		3	KP.4, ÖS.2, PR.2
Güvenirlilik		3	KP.4, ÖS.1, PR.2
Toplumsal ve ulusal güvenlik		5	KP.1, KP.2, ÖS.1, ÖS.2, PR.1
	Stratejik iletişim	6	KP.1, ÖS22, ÖS.3, PR.1, PR.2, PR.3
	İstihbari bilgilerin sızdırılması	2	KP.2, ÖS.1
	Sınırlı düzeyde veri ve bilgi aktarımı	1	KP.1
	Ülke politikalarına müdahale	1	ÖS.2
	İsyan, dezenformasyon vb.	1	ÖS.1

Tablo 3. "Savaş ve barış dönemi" temasının kodları, frekansları ve katılımcıları

Katılımcılar, bilgi, iletişim ve haberleşme teknolojileri şirketlerinin savaş ve barış dönemlerindeki önemine dair görüşlerini farklı açılardan değerlendirmişlerdir. Dokuz katılımcı, bankacılık, finans, sağlık, enerji ve eğitim gibi kritik kamu hizmetlerinin kesintisiz sürdürülebilmesi için bu şirketlerin hayati rol oynadığını belirtmiştir. Sekiz katılımcı, bu şirketlerin ulusal güvenlik açısından stratejik bir öneme sahip olduğunu vurgulamıştır. Üç katılımcı, şirketlerin siber direnç kapasitesi ve üretim gücüne dikkat çekerek, kriz dönemlerinde altyapılarda oluşabilecek güvenlik tehditlerine karşı çözüm, direnç ve derinlik sağladığını ifade etmiştir. Ayrıca, üç katılımcı, savaş dönemlerinde bu şirketlerin tarafsızlık ve güvenilirlik ilkelerine bağlı kalmasının kritik olduğunu vurgulamış ve güvenilir şirketlerin tercih edilmesi gerektiğini belirtmiştir.

> **KP.1.:** "Savaş, barış, afet ve kriz dönemlerinde iletişim, kamu hizmetlerinin devamlılığı, toplum sağlığı ve güvenliği ve ulusal güvenlik hayati öneme sahiptir. 20 Şubat 2023 tarihinde yaşadığımız deprem felaketinde, 15 Temmuz hain FETÖ darbe girişimi süreçlerinde ses ile haberleşmek mümkün olmadı. Bu noktada haberleşme ve iletişim altyapısının direnci olmazsa olmazımız. Bilgi, iletişim ve haberleşme teknolojileri şirketleri bahse konu süreçlerde iletişimin devamlılığını sağlamakla yükümlüdür."

> **KP.3.:** "21. yüzyılda bilgi ve iletişim teknolojileri, devletlerin kılcal damarlarına benzetilebilir. Sanayi, bankacılık, sağlık ve eğitim gibi temel sektörler bu bilgi, iletişim teknolojileri altyapısına

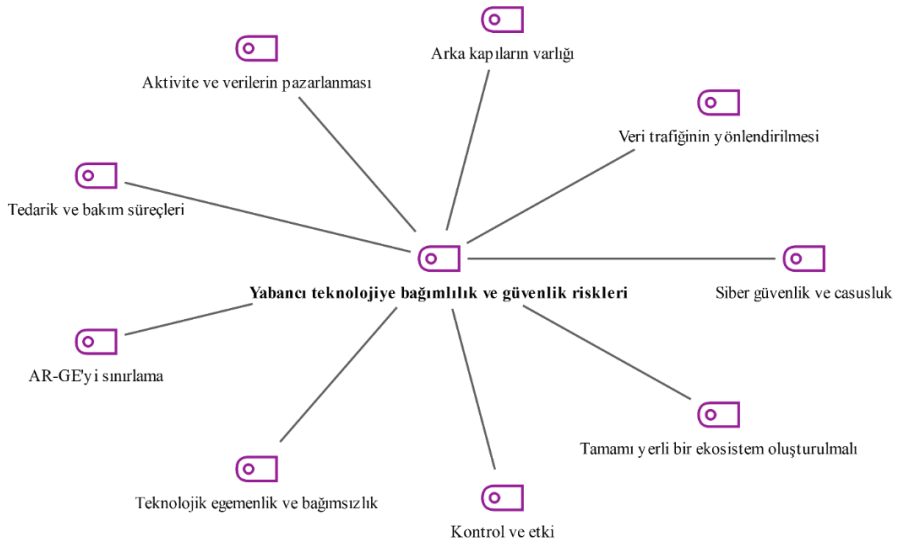
bağımlıdır. Hem savaş hem de barış dönemlerinde bu altyapıların sağlıklı çalışması hayati öneme sahiptir."

ÖS.2.:"Savaş veya çatışma tehdidinin bulunduğu dönemlerde sizin iletişim altyapılarınız düşmanınız için stratejik hedefler olarak belirlenir. Bu kapsamda hizmet alınan bilgi ve iletişim teknolojisi şirketinin size sunacağı çözümler, direnç ve derinlik oldukça önemlidir. Günümüzde küreselleşmenin getirdiği en önemli toplumsal sonuçlardan birisi anlık ve çok çeşitli iletişim kaynaklarıdır. Bu noktada kısıtlı süre için de olsa iletişim kanallarınızın devre dışı kalması siyasi otoritenin sarsılması gibi çeşitli sonuçlar açığa çıkartır."

PR.1.: "Savaş zamanlarında bu şirketler; iletişim altyapısının işlerliğini sürdürmek, acil durum hizmetlerini desteklemek ve stratejik iletişimi sağlamak için temel rol oynar. Barış dönemlerinde ise, ekonomik büyüme, eğitim, sağlık hizmetleri ve toplumsal bağlantılılık gibi alanlarda temel bir altyapı sağlayarak toplumun genel refahına katkıda bulunurlar. Her iki dönemde de bu şirketlerin sağladığı hizmetler, toplumun işleyişi ve güvenliği için merkezi önem taşır."

(iii) Yabancı teknolojiye bağımlılık ve güvenlik riskleri

Katılımcılar, bilgi, iletişim ve haberleşme teknolojileri altyapısı, ekipman ve donanımlarında yabancı teknolojiye bağımlılığın doğurabileceği potansiyel güvenlik risklerini değerlendirmiştir; bu bulgular Şekil 6 ve Tablo 4'te sunulmuştur.



Şekil 6. "Yabancı teknolojiye bağımlılık ve güvenlik riskleri" temasının kodları

Kodlar	Frekans	Katılımcılar
Siber güvenlik ve casusluk	10	KP.2, KP.3, KP.4, ÖS.1, ÖS.3, ÖS.4. ÖS.5, PR.1, PR.2, PR.3
Tamamı yerli bir ekosistem oluşturulmalı	4	KP.1, ÖS.1, ÖS.2, PR.1
Kontrol ve etki	2	ÖS.1, PR.2
Teknolojik egemenlik ve bağımsızlık	2	ÖS.2, PR.3
AR-GE'yi sınırlama	2	KP.3, ÖS.2
Tedarik ve bakım süreçleri	2	KP.2, PR.2
Aktivite ve verilerin pazarlanması	2	KP.1, PR.2
Veri trafiğinin yönlendirilmesi	1	KP.1
Arka kapıların varlığı	1	KP.1

Tablo 4. "Yabancı teknolojiye bağımlılık ve güvenlik riskleri" temasının kodları, frekansları ve katılımcıları

Katılımcılar, yabancı teknolojiye bağımlılığın doğurabileceği siber güvenlik ve ulusal güvenlik risklerine dikkat çekmiştir. On katılımcı, kritik altyapılar, kamu güvenliği, askeri sistemler ve finans sektörlerinin siber casusluk, veri yönlendirme ve arka kapı erişimi gibi tehditlerle karşı karşıya kalabileceğini vurgulamıştır. İki katılımcı, bağımlılığın ulusal egemenlik ve teknolojik bağımsızlık açısından risk oluşturduğunu ifade ederken, iki katılımcı ise yerli AR-GE yatırımlarını sınırlayabileceğini belirtmiştir. İki katılımcı, kriz dönemlerinde tedarik zinciri kesintilerinin yaşanabileceğine dikkat çekmiş, dört katılımcı ise yerli bir teknoloji ekosisteminin oluşturulmasının gerekliliğini vurgulamıştır.

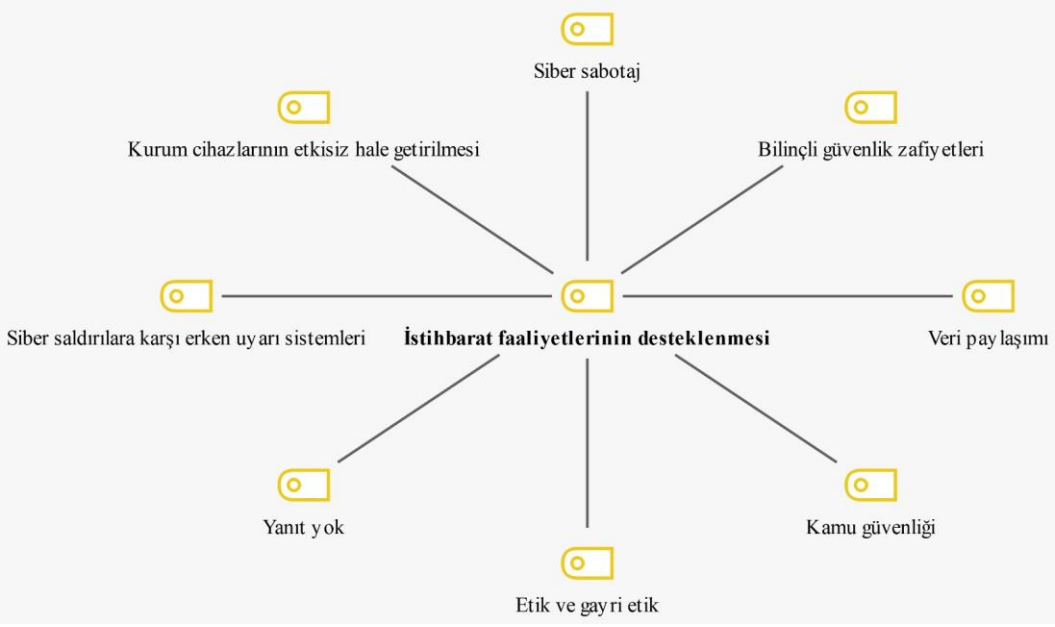
> **ÖS.5:** "Siber savaş olarak isimlendirdiğimiz kavram hibrit savaşın önemli bir bileşenidir. Bilgi iletişim teknolojileri ve bu teknolojilere bağlı hizmetlerde dışa bağımlılık savaş alanında negatif yönlü bir güç çarpanıdır. Özellikle BİHT tedarik edilen bir aktör ile çatışma/savaş durumunun yaşanması durumunda sistemleriniz üzerinden casusluk ve sistemlerinize yönelik siber sabotaj riski bulunur."

> **KP.3.:** "Yabancı teknolojiye bağımlılık birçok sorunu beraberinde getirir. Öncelikle ülkenin yüksek teknoloji alanında AR-GE'ye ayrılan bütçenin azalmasına neden olabilir. Siber güvenlik boyutunda ise; hizmet sağlayıcı şirkete gerçekleştirilebilecek 3. taraf saldırılardan müşteriler de etkilenebilir. Buna ek olarak; politik ilişkiler de bu durumu şekillendirerek siber güvenlik riskleri açığa çıkabilir.

> **KP.1.:** "Tüm şirketlerin ekipmanlarında arka kapılar bıraktığına inanıyorum. Özellikle temel kaynak kodlarına erişmenin mümkün olmadığı yazılım ve donanımlarda için bu riski değerlendirmek mümkün olmuyor. Kurumsal ve/veya bireysel olarak sisteminiz için bütün güvenlik önlemlerini alsanız dahi hizmet aldığınız kurumlar verilerinizi yönlendirebiliyor. Bu durum spesifik olarak bir tek şirket için geçerli değildir. Sektördeki birçok şirket veri trafiğini kendi tasarruflarına göre yönlendirmektedir. Bilgi, iletişim ve haberleşme teknoloji şirketleri hemen hemen her aktivitenizi kayıt altına alıyor. Aktivite ve verilerinizi pazarlıyor. Bu ve benzeri tehditlerin önüne geçilmesi için bilişim güvenlik sistemlerine yönelik AR-GE kapasitesinin arttırılması ve tamamı ile yerli bir ekosistem yaratmanın gerekli olduğunu düşünüyorum."

(iv) İstihbarat faaliyetlerinin desteklenmesi

Katılımcılar, bilgi, iletişim ve haberleşme teknolojileri şirketlerinin hükümetler ve kolluk kuvvetleri tarafından istihbarat faaliyetlerini desteklemek amacıyla nasıl kullanılabileceğine dair görüşlerini paylaşmışlardır. Bu değerlendirmeler Şekil 7 ve Tablo 5'te sunulmuştur.



Şekil 7. "İstihbarat faaliyetlerinin desteklenmesi" temasının kodları

Kodlar	Frekans	Katılımcılar
Yanıt yok	3	KP.4, ÖS.4, PR.2
Veri paylaşımı	8	KP.1, KP.3, ÖS.1, ÖS.2, ÖS.3, ÖS.5, PR.1, PR.3
Kamu güvenliği	4	KP.2, ÖS.2, ÖS.3, PR.1
Etik ve gayri etik	3	KP.2, PR.1, PR.3
Bilinçli güvenlik zafiyetleri	1	ÖS.3
Siber saldırılara karşı erken uyarı sistemleri	1	ÖS.2
Kurum cihazlarının etkisiz hale getirilmesi	1	ÖS.5
Siber sabotaj	1	KP.1

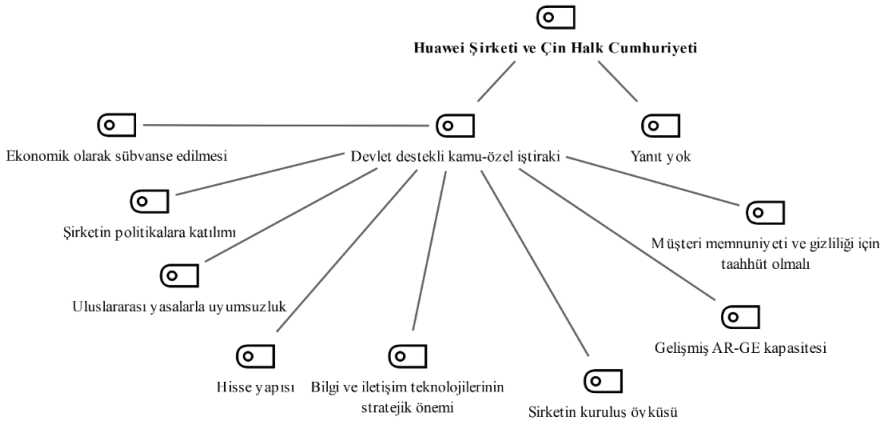
Tablo 5. "İstihbarat faaliyetlerinin desteklenmesi" temasının kodları, frekansları ve katılımcıları

Üç katılımcı, bilgi, iletişim ve haberleşme teknolojileri şirketlerinin hükümetler ve kolluk kuvvetlerinin istihbarat faaliyetlerini nasıl destekleyebileceğine dair görüş bildirmemiştir. Sekiz katılımcı, bu şirketlerin konum bilgileri, iletişim kayıtları ve sosyal medya aktivitelerini paylaşarak istihbari destek sağlayabileceğini ifade etmiştir. Dört katılımcı, bu verilerin terörle mücadele ve kamu güvenliğinin sağlanması için kullanılabileceğini belirtirken, üç katılımcı mahremiyet ve ulusal güvenlik dengesine dikkat çekmiştir. Ayrıca, siber saldırılara karşı erken uyarı sistemlerinin geliştirilmesi ve hedef cihazların etkisiz hale getirilmesi gibi alanlarda şirketlerin istihbari işlev görebileceği vurgulanmıştır. Öte yandan, bazı katılımcılar şirketlerin hizmet verilen ülkeye karşı siber sabotaj, hizmet kesintisi ve veri sızıntısı riski taşıdığına dikkat çekmiştir.

> **ÖS.3.:** "Bir diğer ihtimal ise; bilgi ve iletişim teknolojileri şirketinin hizmet sağladığı ülkeye karşı bir faaliyet yürütmesidir. Bu durum da şirket menşei olduğu bağlı bulunduğu ülkenin çıkarları doğrultusunda hizmet sağladığı ülke de bilinçli olarak çeşitli güvenlik zafiyetleri oraya çıkarması ile gerçekleşir. Veri sızıntıları, iletişim altyapısında bilinçli kesintiler ve siber sabotaj yöntemleri burada ön plana çıkar. Özellikle istihbarat niteliği taşıyan sözel istihbarat verileri, harekât planları ve önemli endüstriyel projelerin sızdırılması bunlara örnektir."
>
> **PR.3.:** "BİHT şirketleri hükümetlerin ve kolluk kuvvetlerinin istihbarat faaliyetlerini desteklemek için kullanılabilir ve bu kişisel mahremiyet ve etik gibi bazı endişeler oluşturuyor. BİHT şirketleri, yasal olarak suç takibi amacıyla istihbarat faaliyetlerini desteklemek için kullanıcıların konum verilerini ve iletişim bilgilerini kolluk kuvvetleriyle paylaşabilir."
>
> **KP.2.:** "Bu sorunun etik ve gayri etik iki boyutu olduğunu düşünüyorum. Etik boyutu; bir ülkenin terörizmle mücadele, suç önleme, suçlu yakalama gibi kamu güvenliği ve toplum huzurunu önceleyen ve belirli bir hukuk çerçevesinde ele alınan bir tarafı vardır. Suçlunun iletişiminin dinlenmesi, yer tespitinin yapılması hukuk organlarınca izin verildiği müddetçe etiktir. Etik olmayan boyutu ise; yabancı hükümetlerle ve yabancı istihbarat örgütleriyle iş birliği durumunda ortaya çıkar. Burada şirketlerin iş birliğine bakış açıları, bağlı oldukları yasa ve kanunlar önemlidir."

(v) Huawei Şirketi ve Çin Halk Cumhuriyeti

Katılımcılar, Huawei Şirketi'nin Çin hükümeti ile ilişkisi ve kamu-özel iş birliği modeliyle çalışıp çalışmadığı konusundaki görüşlerini paylaşmışlardır. Bu değerlendirmeler Şekil 8 ve Tablo 6'da sunulmuştur.



Şekil 8. "Huawei Şirketi ve Çin Halk Cumhuriyeti" temasının kodları

Kodlar	**Alt kodlar**	**Frekans**	**Katılımcılar**
Yanıt yok		2	KP.4, ÖS.1
Devlet destekli kamu-özel iştiraki		10	KP.1, KP.2, KP.3, ÖS.2, ÖS.3, ÖS.4, ÖS.5, PR.1, PR.2, PR.3
	Ekonomik olarak sübvanse edilmesi	3	ÖS.2, ÖS.3, ÖS.5
	Şirketin politikalara katılımı	3	KP.2, ÖS.3, PR.2
	Uluslararası yasalarla uyumsuzluk	1	PR.3
	Hisse yapısı	1	PR.2
	Şirketin kuruluş öyküsü	1	PR.1
	Bilgi ve iletişim teknolojilerinin stratejik önemi	1	KP.3
	Müşteri mahremiyeti ve gizliliği için taahhüt olmalı	1	KP.1
	Gelişmiş AR-GE kapasitesi	1	KP.1

Tablo 6. "Huawei Şirketi ve Çin Halk Cumhuriyeti" Temasının Kodları, Frekansları ve Katılımcıları

İki katılımcı, Huawei Şirketi'nin Çin hükümetine bağlı bir kamu-özel iştiraki olup olmadığına dair görüş bildirmezken, on katılımcı şirketin doğrudan devletle bağlantılı olduğunu ifade etmiştir. Katılımcılar, Huawei'nin devlet sübvansiyonları ile desteklenmesi, Çin'in uluslararası politikalarındaki rolü, hisse yapısındaki belirsizlik, kuruluş süreci ve büyüme stratejileri, bilgi ve iletişim teknolojilerinin Çin hükümeti için stratejik önemi ve şirketin güçlü AR-GE kapasitesi gibi faktörleri bu değerlendirmeye gerekçe olarak göstermiştir. Bir katılımcı ise, kamu-özel iştiraki olarak konumlanan bir şirketin müşteri mahremiyeti ve veri gizliliği konularında daha fazla taahhütte bulunması gerektiğini vurgulamıştır.

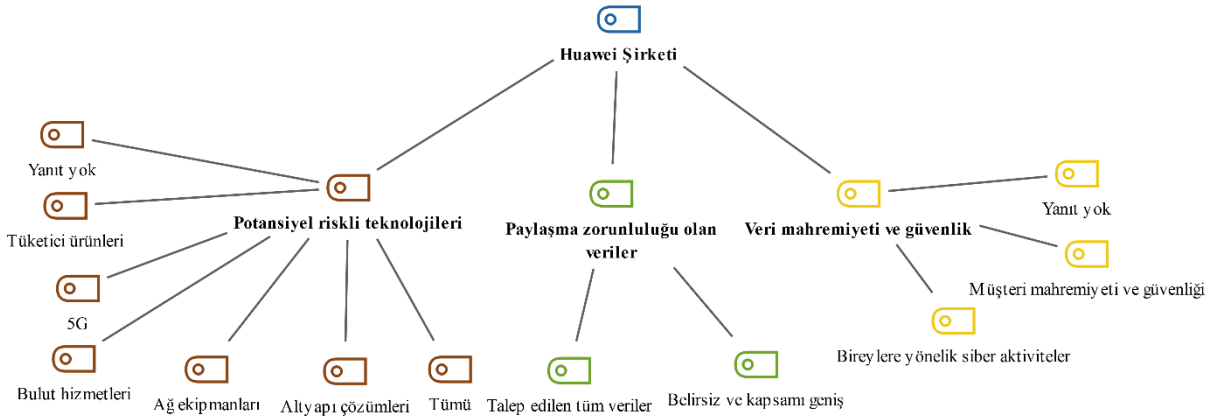
> **PR.3.:** "Söz konusu Çin olunca yüksek teknoloji ürünleri üreten birçok firma kamu-özel iştirakidir. Huawei'nin durumu da tam olarak bu. Çin Halk Cumhuriyeti'nin anayasal düzeni özellikle insan hakları ve mahremiyet noktasında uluslararası standartlarla çelişkilidir. Bu durum, Huawei şirketinin bağımsızlığı ve uluslararası yasalara olan bağlılığı konusunda çok ciddi şüpheler uyandırır."

> **ÖS.3.:** "Huawei Şirketi'nin bu durumunu tartışırken şirketin iş modelleri, büyüme stratejileri ve uluslararası genişlemesi de göz önünde bulundurulması gerektiğini düşünüyorum. Bunu ifade ederken; Çin Halk Cumhuriyeti'nin dijital ipek yolu projesi gibi bilgi ve iletişim teknolojileri ile yakın ilişkili projelerinde şirketin oynadığı role de bakmak gerekiyor. Bu farklı bir bakış açısıyla değerlendirmeye de olanak sunuyor. Şirket bu projeleri gerçekleştirirken ne kadar devlet sübvansiyonu almış, şirketin kurucusu askeri bir mühendisken şirket çokta uzun olmayan bir süre

içerisinde nasıl bu kadar büyümüş hepsi ayrı tartışma konuları. Tüm bunları dikkate aldığımda Şirketin keskin bir biçimde Çin Hükümeti ve Komünist Parti ile ilişkili olduğunu ifade edebilirim."

(vi) Huawei Şirketi ve Ulusal İstihbarat Yasası

Katılımcılar, ÇHC Ulusal İstihbarat Yasası'nın 7. Maddesi kapsamında Huawei Şirketi'nin Çin hükümeti ile hangi verileri paylaşmakla yükümlü olabileceğine, Huawei ile Çin hükümeti arasındaki ilişkinin müşteri verilerinin mahremiyeti ve güvenliği üzerindeki etkilerine ve Huawei'nin hangi teknolojilerinin potansiyel olarak güvenlik riski taşıdığına dair görüşlerini ifade etmişlerdir. Bu değerlendirmeler, Şekil 9 ve Tablo 7'de detaylandırılmıştır.



Şekil 9. "Huawei Şirketi" teması, alt temaları ve kodları

Alt temalar	Kodlar	Frekans	Katılımcılar
Paylaşma zorunluluğu olan veriler	Belirsiz ve kapsamı geniş	10	KP.2, KP.3, ÖS.1, ÖS.2, ÖS.3, ÖS.4, ÖS.5, PR.1, PR.2., PR.3
	Talep edilen tüm veriler	11	KP.1, KP.2, KP.3, KP.4, ÖS.1, ÖS.2, ÖS.3, ÖS.4, ÖS.5, PR.2, PR.3
Veri mahremiyeti ve güvenlik	Yanıt yok	4	KP.4, ÖS.1, ÖS.2, ÖS.5
	Müşteri mahremiyeti ve güvenliği	7	KP.1, KP.3, ÖS.3, ÖS.4, PR.1, PR.2, PR.3
	Bireylere yönelik siber aktiviteler	2	KP.2, ÖS.4
Potansiyel riskli teknolojileri	Yanıt yok	1	KP.4
	Tüketici ürünleri	6	KP.2, ÖS.2, ÖS.5, PR.1, PR.2, PR.3
	Altyapı çözümleri	5	ÖS.2, ÖS.3, ÖS.5, PR.1, PR.2
	Ağ ekipmanları	4	KP.1, KP.3, ÖS.1, ÖS.3
	5G	3	KP.2, ÖS.4, PR.3
	Bulut hizmetleri	2	ÖS.2, PR.1
	Tümü	1	ÖS.2

Tablo 7. "Huawei Şirketi" temasının alt temaları kodları, frekansları ve katılımcıları

On bir katılımcı, Huawei Şirketi'nin Çin Hükümeti tarafından talep edilen tüm verileri paylaşmakla yükümlü olduğunu belirtirken, on katılımcı, Ulusal İstihbarat Yasası'nın 7. Maddesi'nin muğlak bir yapıya sahip olduğunu, kapsadığı sektörlerin geniş bir çerçevede değerlendirildiğini ve uygulanma biçiminin belirsizlik taşıdığını ifade etmiştir.

KP.3.: "İlgili maddelerde hangi koşullarda hangi verilerin paylaşılacağı açıkça belirtilmemiş. Bu durum ortada büyük bir belirsizlik yaratıyor. Benim buradaki çıkarımım talep edilen bütün verilerin paylaşılmak zorunda olduğudur."

ÖS.5.: "Kanunda genel olarak ülkede bulunan tüm kuruluşlar işaret edilmektedir. Bir istihbarat bilgisi talep edilmesi durumunda verilerin paylaşılacağını anlıyorum. Açık kaynak istihbaratı

özelinde konuşmak gerekirse; bir kullanıcının dijital ayak izi, fotoğraf, IP adresleri önemli verilerdir. Fakat bazı durumlarda bir fotoğraf karesi bile önemli bir ipucu olabiliyor. Dolayısıyla, hangi bilginin/verinin istihbarata katkı sunacağı belirsizdir. Sonuç olarak, tüm veriler istihbarat için kullanılabilir ve hükümetin hangi veriyi talep edeceği belirsizdir."

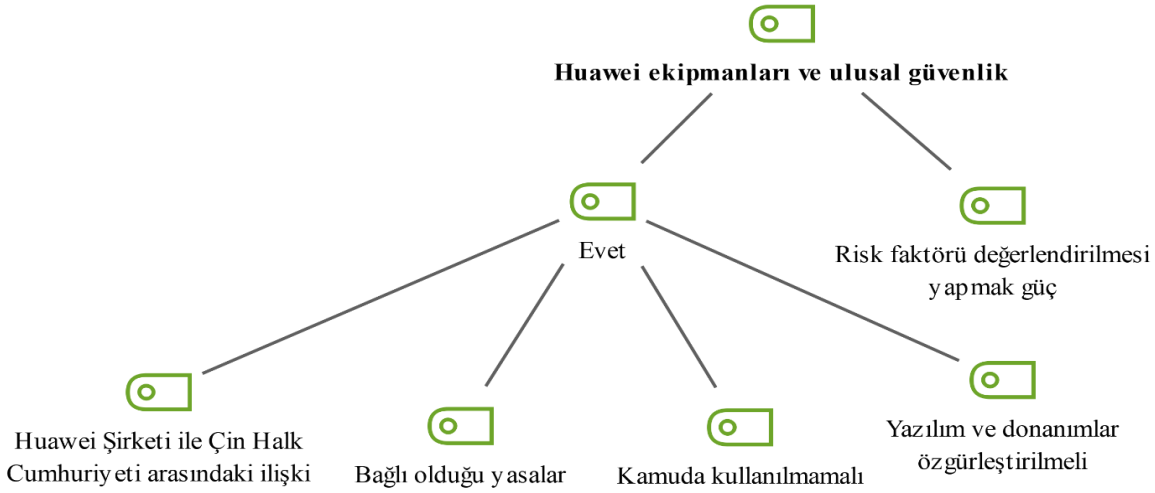
Yedi katılımcı, müşteri mahremiyeti ve güvenliğine yönelik risklerin, özgürlüklerin kısıtlanmasına kadar varabilecek tehditler oluşturduğunu belirtmiştir. İki katılımcı ise bireyleri hedef alabilecek olası siber faaliyetlere dikkat çekmiştir.

ÖS.4.: *"Müşterilerin mahremiyeti sözleşme ve yasalarla korunmaktadır. Ancak, Çin Hükümeti ve Huawei Şirketi arasındaki ilişkinin sınırları belirsizdir. Mahremiyet ve güvenlik bağlamında potansiyel bir risk teşkil etmektedir."*

PR.2.: "Varlığı kabul edilen bu ilişkinin boyutu bizlere müşteri verilerinin tümünün talep edilmesi noktasında paylaşılmak zorunda olduğunu gösteriyor. Burada bireysel kullanıcıların mahremiyeti, kurumsal kullanıcıların ise güvenlik, sır ve mahremiyetleri tehdit altındadır. Bu veriler arasında; ticari ve teknolojik sırlardan hizmetlerin kullanım alanına göre askeri sırlara birçok veriden söz etmek mümkündür."

(vii) Huawei ekipmanları ve ulusal güvenlik

Katılımcılar, Huawei ekipmanlarının ulusal güvenlik açısından oluşturabileceği risklere dair değerlendirmelerini aktarmışlardır. Bu değerlendirmeler, Şekil 10 ve Tablo 8'de sunulmuştur.



Şekil 10. "Huawei ekipmanları ve ulusal güvenlik" temasının kodları

Kodlar	Alt kodlar	Frekans	Katılımcılar
Risk faktörü değerlendirilmesi yapmak güç		1	PR.1
Evet		11	KP.1, KP.2, KP.3, KP.4, ÖS.1, ÖS.2, ÖS.3, ÖS.4, ÖS.5, PR.2, PR.3
	Huawei Şirketi ile Çin Halk Cumhuriyeti arasındaki ilişki	5	KP.1, KP.2, ÖS.5, PR.2, PR.3
	Bağlı olduğu yasalar	2	KP.3, ÖS.5
	Kamuda kullanılmamalı	1	KP.4
	Yazılım ve donanımlar özgürleştirilmeli	1	KP.1

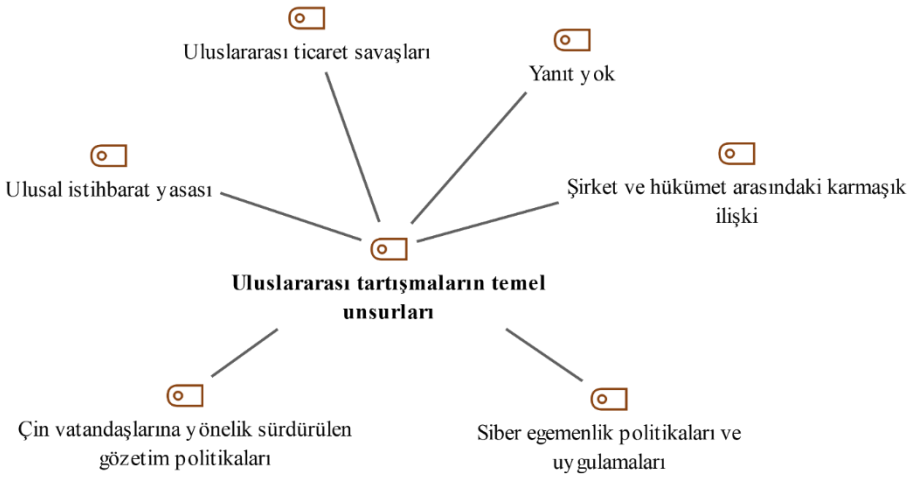
Tablo 8. *"Huawei ekipmanları ve ulusal güvenlik" temasının kodları, frekansları ve katılımcıları*

Bir katılımcı, Huawei ekipmanlarının ulusal güvenlik için oluşturduğu riskin kesin olarak değerlendirilmesinin zor olduğunu belirtirken, diğer tüm katılımcılar bu ekipmanların risk teşkil ettiğini ifade etmiştir. Katılımcılar, ekipmanın kullanıldığı alan ve fonksiyonuna bağlı olarak risk seviyesinin arttığını vurgulamışlardır. Bu durumun temel nedenleri arasında, Huawei Şirketi ile ÇHC arasındaki karmaşık ilişki ve şirketin tabi olduğu yasalar gösterilmiştir. Bu nedenle, kamu kurumlarında Huawei'ye ait bilgi teknolojilerinin kullanımından kaçınılması ve yazılım ile donanımda bağımsızlığın sağlanması gerektiği ifade edilmiştir.

> **KP.1.:** "Evet Huawei Şirketi idari yapısı ve Çin Halk Cumhuriyeti devletinin politikaları nedeni ile özellikle kamu kurumları ve kritik altyapılarda kullanılması risk teşkil ediyor. Ancak bu noktada yalnızca Huawei Şirketi'nin ürünleri değil piyasada bulunan yabancı menşeli tüm ürünler risk teşkil ediyor. Türkiye'de birçok altyapıda kullanılan ürünlerin tedarikçisinin Huawei Şirketi olduğu da bilinen bir gerçek. Bu noktada kullanılan yazılım ve donanımların özgürleştirilmesinin gerektiği düşüncesindeyim. Kamu kurumlarında kullanılan yabancı menşeli bilgi, iletişim ve haberleşme teknolojileri ekipmanlarının tedarikçi firma ile anlaşma sağlama koşulu ile kripto analistlerin ve kriptologların ortak çalışması ile güvence altına alınabileceği düşüncesindeyim."
>
> **ÖS.5.:** "Yüzde yüz güvenlikten veya yüzde yüz tehditten bahsetmek mümkün değildir. Huawei Şirketi'nin Çin Halk Cumhuriyeti sınırları dışında vermiş olduğu hizmetlerde hangi standartlara bağlı kalacağı belirleyicidir. Bu yüzden kısmen risk teşkil edeceği düşüncesindeyim."
>
> **KP.3.:** "Burada bir ayrım yapmak gerekiyor. Huawei Şirketi'nin ekipmanları belki tek başına güvenlik riski oluşturmaz. Ancak, bağlı olduğu yasalar itibariyle kısmen risk teşkil eder."
>
> **PR.1.:** "Bu konuda net bir yanıt vermenin mümkün olmadığını düşünüyorum. Burada bir risk faktörü değerlendirmesi yapmak birçok faktöre bağlıdır. Huawei ekipmanlarının ulusal güvenlik için potansiyel bir risk teşkil edip etmediği, güvenlik önlemleri, ürünlerin güvenlik açıklarına karşı güncellenme sıklığı, ekipmanların kritik altyapılarda kullanımı, ulusal ve uluslararası güvenlik standartlarına uyumu ve üretici firmanın hükümetle ilişkileri yer alır. Bu faktörler, bir ülkenin ulusal güvenliği açısından potansiyel risklerin kapsamını ve şiddetini belirlemede önemlidir. Her bir durum, bu çeşitli faktörlere bağlı olarak ayrı ayrı değerlendirilmelidir. Bazı ülkeler ve kurumlar, güvenlik endişeleri nedeniyle Huawei teknolojilerinin kullanımını sınırlandırmış veya yasaklamıştır, bu da konunun karmaşıklığını ve çeşitli perspektiflerden değerlendirilmesi gerektiğini göstermektedir."

(viii) Uluslararası tartışmaların temelleri

Çalışmanın katılımcıları, Huawei Şirketi ve sunduğu hizmetlerin uluslararası düzeyde tartışmalı hale gelmesine neden olan temel unsurları değerlendirmişlerdir. Bu değerlendirmeler, Şekil 11 ve Tablo 9'da detaylı olarak sunulmuştur.



Şekil 11. "Uluslararası tartışmaların temel unsurları" temasının kodları

Kodlar	Frekans	Katılımcılar
Yanıt yok	2	KP.4, ÖS.1
Şirket ve hükümet arasındaki karmaşık ilişki	6	ÖS.2, ÖS.4, ÖS.5, PR.1, PR.2, PR.3
Siber egemenlik politikaları ve uygulamaları	5	KP.2, ÖS.2, ÖS.3, ÖS.4, PR.2
Ulusal istihbarat yasası	3	KP.2, KP.3, ÖS.3
Çin vatandaşlarına yönelik sürdürülen gözetim politikaları	2	ÖS.2, ÖS.3
Uluslararası ticaret savaşları	2	KP.1, PR.1

Tablo 9. "Uluslararası tartışmaların temel unsurları" temasının kodları, frekansları ve katılımcıları

İki katılımcı, Huawei Şirketi ve hizmetlerinin uluslararası alanda tartışmalı hale gelmesine ilişkin görüş bildirmezken, altı katılımcı şirketin tartışmalı hisse yapısı ve Çin hükümetiyle olan karmaşık ilişkisine dikkat çekmiştir. Beş katılımcı, Çin'in siber egemenlik politikaları ve uygulamalarının Huawei üzerindeki etkisini vurgularken, üç katılımcı Ulusal İstihbarat Yasası'nın belirsizliği nedeniyle şirketin güvenilirliğinin sorgulandığını ifade etmiştir. Ayrıca, iki katılımcı Çin vatandaşlarına yönelik gözetim politikalarının şirketin uluslararası imajını olumsuz etkilediğini, iki katılımcı ise Huawei'nin küresel düzeyde tartışmalı hale gelmesinde uluslararası ticaret savaşlarının belirleyici bir faktör olduğunu belirtmiştir.

> **KP.2.:** "Kuşkusuz Çin Komünist Partisi ve Huawei Şirketi arasındaki ilişki Huawei Şirketi'nin hizmetlerini tartışmalı hale getirmektedir. Şirket'in Çin Hükümeti adına kullanışlı bir apart olduğu kanaatindeyim. Bu kanaate varmamda kuşkusuz ulusal istihbarat yasası ve Çin Halk Cumhuriyeti'nin siber egemenlik politikalarında şirkete düşen rol etkili olmuştur."
>
> **ÖS.2.:** "Ulusal istihbarat yasasından bağımsız olarak düşünüldüğünde; Huawei Şirketi'nin hisseli yapısı tartışmalıdır. Çin Komünist Partisi kâğıt üzerinde olmasa da dolaylı olarak şirketin sahibidir. Çin devleti siber gözetim noktasında oldukça mahir bir ülkedir. Kendi nüfusu üzerinde uyguladığı uygulamalar, uluslararası alanda yapacağı uygulamaların bir örneğini teşkil etmektedir. Bu noktada şeffaflık ve güvenlik meseleleri şirketi tartışmalı hale getiren baskın etmenlerdir."
>
> **PR.2.:** "Çin Halk Cumhuriyeti'nin nüfusu ve yönetim yapısı düşünüldüğünde gözetim teknolojileri geliştirme ve pratik uygulamalarında tasvip etmesem de oldukça başarılıdır. Çin teknolojilerinin özellikle NATO ülkelerinin askeri ve kritik altyapılarına entegre edilmesi tüm blok için tehdit oluşturmaktadır. Çin Halk Cumhuriyeti siber istihbarat ve siber saldırı noktasında hem sivil hem de askeri olarak yapılar inşa etmiştir. Bu yapılar aracılığıyla düşman aktörlere yönelik oldukça maliyetli saldırılar gerçekleştirebilmektedir. Huawei Şirketi'nin de Çin devleti ile olan ilişkisi, Şirketi potansiyel bir tehdit öznesi haline getirmektedir."

Tartışma ve sonuç

David Kahn, istihbarat kaynaklarının tarihsel süreçte çeşitlendiğini ifade etmektedir. 21. yüzyılda bilgi, iletişim ve haberleşme teknolojilerindeki hızlı gelişmeler, sözel istihbarat verilerinin artışını hızlandırmış ve bilgi teknolojileri şirketlerini önemli istihbarat kaynakları haline getirmiştir. Günümüzde kritik altyapılar, bankacılık, sağlık, finans, eğitim ve kamu hizmetleri büyük ölçüde bilgi ve iletişim teknolojilerine bağımlı hale gelmiş olup, bu teknolojilerin güvenliği, ulusal güvenlik açısından stratejik bir öneme sahiptir.

Bu çalışma, Huawei Şirketi ile Çin Halk Cumhuriyeti'nin istihbarat ve güvenlik servisleri arasındaki ilişkiyi inceleyerek, bu bağlantının karşı istihbarat bağlamında doğurabileceği sorunları değerlendirmektedir. Araştırma bulguları, Huawei'nin Çin devlet politikalarının bir parçası olarak konumlandığını ve bu durumun uluslararası güvenlik dinamikleri açısından riskler barındırdığını göstermektedir. Şirketin kuruluş sürecinden itibaren Çin devlet bankaları tarafından desteklenmesi, finansal teşviklerle büyütülmesi ve devletin teknoloji politikaları ile paralel hareket etmesi, Huawei'nin bir kamu-özel iştiraki olarak faaliyet gösterdiği yönündeki iddiaları güçlendirmektedir.

Huawei, hisselerinin tamamının çalışanlarına ait olduğunu öne sürmektedir, ancak Çin'deki yasal düzenlemeler doğrultusunda, bir şirketin 50'den fazla hissedarı olamayacağı için bu hisseler sendika bünyesinde toplanmaktadır. Ancak, söz konusu sendikanın doğrudan ÇKP tarafından denetlenmesi, şirketin bağımsız bir özel girişim olduğu iddialarını zayıflatmaktadır. Araştırma bulguları, Huawei'nin Çin hükümetine hukuki olarak bağlı olduğu ve hükümetin talepleri doğrultusunda istihbarat ve veri paylaşmak zorunda kalabileceğini ortaya koymaktadır. Ulusal İstihbarat Yasası'nın muğlak yapısı, Huawei'nin Çin devleti tarafından küresel bilgi akışını kontrol etmek ve siber egemenlik stratejilerini güçlendirmek için kullanılabileceğine dair endişeleri artırmaktadır.

Yarı yapılandırılmış görüşmelerden elde edilen bulgular, bilgi, iletişim ve haberleşme teknolojileri şirketlerinin istihbarat faaliyetlerini destekleme biçimlerinin iki ana kategoriye ayrılabileceğini göstermektedir. İlk olarak, terörle mücadele, iç güvenlik, suç önleme gibi yasal çerçevede gerçekleştirilen istihbarat destek faaliyetleri, uluslararası hukuka uygun bir şekilde devletlerin güvenlik ihtiyaçlarını karşılamak için yürütülmektedir. İkinci olarak, şirketlerin örtülü operasyonlar ve istihbarat toplama faaliyetleri için kullanılabileceği bulgusu ortaya çıkmıştır. Casusluk, veri sızıntısı, iletişimin dinlenmesi, kritik altyapılara yönelik siber saldırılar ve sistemlerde arka kapı bırakılması gibi faaliyetler, istihbarat savaşlarında bilgi teknolojileri şirketlerinin bir araç olarak kullanılabileceğini göstermektedir.

Çin hükümeti, Ulusal İstihbarat Yasası doğrultusunda ülkede faaliyet gösteren tüm şirketlerin devlet istihbaratına destek vermesini zorunlu kılmaktadır. Araştırmaya katılan uzmanların büyük bir bölümü, Huawei'nin Çin hükümetinin talepleri doğrultusunda bilgi paylaşmak zorunda kalabileceğini ve bu durumun müşteri mahremiyeti açısından ciddi riskler taşıdığını ifade etmektedir. Huawei'nin 5G ve telekomünikasyon altyapılarındaki etkisi, şirketin sadece bir teknoloji sağlayıcısı olmadığını, aynı zamanda Çin devletinin küresel istihbarat stratejisinin bir parçası olarak konumlandığını göstermektedir.

Bu çalışmanın bir diğer amacı, bilgi, iletişim ve haberleşme teknolojileri şirketlerinin bir karşı istihbarat sorunu haline nasıl gelebileceğini ortaya koymaktır. Bu tür şirketlerin güvenilirliği ve uluslararası güvenlik standartlarına bağlılıkları, devletlerin bilgi ve iletişim teknolojileri politikalarını şekillendirmede kritik bir unsur haline gelmiştir. Huawei örneği, bir teknoloji şirketinin nasıl uluslararası güvenlik tartışmalarının merkezine yerleşebileceğini göstermektedir.

Günümüzde bilgi, iletişim ve haberleşme teknolojileri askeri, ekonomik ve siyasi alanlarda kritik bir rol oynamaktadır. Ulusal güvenlik, kamu güvenliği ve kritik altyapılar, doğrudan bu teknolojilere bağımlıdır. İstihbarat topluluklarının faaliyetleri artık yalnızca veri toplamak ve analiz etmekle sınırlı değildir; aynı zamanda siber operasyonlar, sabotaj ve hedef aktörlerin etkisiz hale getirilmesi gibi saldırı stratejilerini de içermektedir. Bu bağlamda, bilgi teknolojileri şirketlerinin yabancı istihbarat faaliyetlerinde nasıl bir araç haline gelebileceği, devletlerin dikkatle değerlendirmesi gereken bir konu haline gelmiştir.

Araştırma bulguları, Huawei'nin Çin devlet politikalarının bir uzantısı olarak hareket edebileceğine ve kritik altyapılar açısından potansiyel güvenlik riskleri taşıdığına işaret etmektedir. Şirketin kamu-özel iştiraki olarak konumlanması, devlet sübvansiyonlarıyla desteklenmesi ve Çin hükümetine bağlı sendikalar tarafından yönetilmesi, bağımsız bir ticari kuruluş olduğu yönündeki iddiaları zayıflatmaktadır. Huawei'nin teknolojik egemenlik ve siber güvenlik bağlamında Çin'in istihbarat stratejileri için önemli bir araç olduğu düşüncesi güçlenmektedir.

Bu kapsamda, devletlerin bilgi, iletişim ve haberleşme teknolojileri tedarik süreçlerinde daha güvenlik odaklı politikalar geliştirmesi gerekmektedir. Türkiye ve diğer ülkeler için kritik altyapı güvenliği açısından yabancı teknoloji bağımlılığının azaltılması, yerli üretimin teşvik edilmesi ve disiplinlerarası güvenlik önlemlerinin uygulanması önerilmektedir. Özellikle 5G teknolojileri ve diğer telekomünikasyon altyapıları söz konusu

olduğunda, Huawei gibi şirketlerin potansiyel tehditleri dikkate alınarak stratejik bir tedarikçi yönetim modeli benimsenmelidir.

Bu çalışma, bilgi, iletişim ve haberleşme teknolojileri şirketlerinin istihbarat faaliyetlerinde nasıl bir rol oynayabileceğini anlamaya yönelik kapsamlı bir çerçeve sunmaktadır. Ancak, konunun dinamik yapısı göz önüne alındığında, gelecek araştırmalarda farklı ülkelerdeki uygulamaların karşılaştırılması, daha geniş örneklem gruplarıyla çalışılması ve Huawei yetkilileriyle doğrudan görüşmeler yapılması, konunun daha derinlemesine anlaşılmasına katkı sağlaması beklenmektedir.

Kaynakça

Alsop, T. (2023). Ranking of telecom infrastructure companies by brand value. Erişim adresi (11 Ocak 2025): https://www.statista.com/statistics/500041/telecom-infrastructure-brand-value/

Amnesty International. (2021). *The Pegasus project report*. London: Amnesty Tech.

Balding, C., & Clarke, D. (2020). *Who owns Huawei?*. Harvard Kennedy School. Cambridge, MA.

Bamford, J. (2002). *Body of secrets: Anatomy of the ultra-secret National Security Agency*. New York: Anchor Books.

Bernhardt, D. (2003). *Competitive intelligence: How to acquire and use corporate intelligence and counter-intelligence*. London: Pearson Education Limited.

Cadwalladr, C. (2019). The Cambridge Analytica files. The Guardian. Erişim adresi (2020): https://www.theguardian.com/news/series/cambridge-analytica-files

Cambridge Dictionary. (2025). Intelligence. Erişim adresi (9 Ocak 2025): https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/intelligence

Creemers, R. (2021). China's conception of cyber sovereignty. *Journal of Cyber Policy*, 6(1), 87-102.

Deibert, R. (2019). *Reset: Reclaiming the internet for civil society*. Toronto: House of Anansi Press.

Demers, J. C. (2018). China's Non-traditional espionage against the United States: The threat and potential policy responses.

Fagel, A. (2020). Cryptographic espionage: The Rubicon case. *Journal of Intelligence Studies*, 23(4), 67-88.

Feldstein, S. (2019). *The global expansion of AI surveillance*. Carnegie Endowment for International Peace. Washington, D.C.

France 24. (2022). What they're doing is called distraction: Chinese spam dilutes Twitter feeds on protests. Erişim adresi (2 Mart 2024): https://observers.france24.com/en/asia-pacific/20221202-what-they-re-doing-is-called-distraction-chinese-spam-dilutes-twitter-feeds-on-zero-covid-protests

Gaddis, J. L. (2002). On strategic surprise. Hoover Digest. Erişim adresi: https://www.hoover.org/research/strategic-surprise

Groll, E. (2020). The spy in your pocket: Mobile surveillance technologies. *Foreign Policy*, 134, 128-144.

Hillman, J., & Sacks, D. (2021). *China's digital silk road: Strategic implications*. Center for Strategic and International Studies. Washington, D.C.

House Permanent Select Committee on Intelligence. (2012). Investigative report on U.S. national security issues posed by Huawei and ZTE.

Huawei. (2021). All Products and Solutions. Erişim adresi (28 Şubat 2023): https://e.huawei.com/en/products-and-solutions/

Inkster, N. (2019). *The Huawei dilemma: Technology and geopolitics*. London: RUSI.

IoT Analytics. (2024). State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally. Erişim adresi (31 Ocak 2025): https://iot-analytics.com/number-connected-iot-devices/

Kahn, D. (2001). An historical theory of intelligence. *Intelligence and national security*, 16(3), 79-92.

Kania, E. B. (2019). *Made in China 2025 and the future of Chinese innovation*. The Brookings Institution. Washington, D.C.

Karmazin, A. (2023). China's promotion of cyber sovereignty beyond the West. Š. Kolmašová & R. Reboredo (Ed.), *Norm diffusion beyond the West: Agents and sources of leverage* (s. 61–76) içinde. Cham: Springer.

Kaska, K., Beckvard, H., & Minárik, T. (2019). *Huawei, 5G and China's National Security Law*. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn.

Kennedy, S. (2018). *China's risky drive into advanced manufacturing*. Center for Strategic and International Studies. Washington, D.C.

Laskai, L. (2018). *Why China's 'Made in China 2025' strategy matters*. Council on Foreign Relations. New York.

Lee, K. (2020). *AI Superpowers: China, Silicon Valley, and the new world order*. Boston: Houghton Mifflin Harcourt.

Lepido, K. (2019). Vodafone found hidden backdoors in Huawei equipment. Bloomberg. Erişim adresi (2021): https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment

Lowenthal, M. M. (2009). *Intelligence: From secrets to policy*. Washington, DC: SAGE Publications.

Marczak, B., Scott-Railton, J., vd. (2021). *NSO Group's Pegasus spyware: A technical analysis*. Citizen Lab.

McCain, J. S. (2018). National defense authorization act for fiscal year 2019 conference report, H.R. 5515, 283.

Pancevski, B. (2020). U.S. officials say Huawei can covertly access telecom networks. The Wall Street Journal. Erişim adresi (5 Mart 2022): https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256

Reuters. (2023). European countries who put curbs on Huawei 5G equipment. Erişim adresi (20 Eylül 2023): https://www.reuters.com/technology/european-countries-who-put-curbs-huawei-5g-equipment-2023-09-28/

Segal, A. (2020). China, cyber sovereignty, and global internet governance. *Foreign Affairs*, 99(3), 113-130.

Steele, R. D. (2007). Open source intelligence. L. K. Johnson (Ed.), *Handbook of intelligence studies* (s. 129-147) içinde. Oxon: Routledge.

Triolo, P., & Webster, G. (2017). *China's cyber governance model*. New America. Washington, D.C.

Triolo, P., Allison, K., & Hillman, J. (2020). *China's digital silk road: Implications for global technology competition*. CSIS Report. Washington, D.C.

Türk Dil Kurumu. (2025). İstihbarat. Erişim adresi (9 Ocak 2025): https://sozluk.gov.tr/

United States District Court Eastern District of New York. (2019, 24 Ocak). *Cr. No. 18-457 (S-2) (AMD)*

Wakabayashi, D., & Rappeport, A. (2018). Huawei CFO Arrested in Canada for extradition to the U.S. New York Times.

Warner, M. (2008). Intelligence as risk shifting. P. Gill, S. Marrin, & M. Phythian (Ed.), *Intelligence theory: Key questions and debates* (s. 54-72) içinde. Oxon: Routledge.

Wen, Y. (2017). The rise of Chinese transnational ICT corporations: The case of Huawei (Yayımlanmamış doktora tezi), Simon Fraser University).

Yıldırım, A., & Şimşek, H. (2021). *Sosyal bilimlerde nitel araştırma yöntemleri*. Ankara: Seçkin Yayıncılık.
Zuboff, S. (2019). *The age of surveillance capitalism*. New York: PublicAffairs.

Araştırmacıların Katkı Oranı: (Birden fazla yazarlı makaleler için)

1. Yazar: % 65

2. Yazar: % 35

Çatışma Beyanı: "Bilgi, iletişim ve haberleşme teknolojileri şirketlerinin istihbarat amaçlı kullanımı: Huawei örneği" isimli makalemiz ile ilgili herhangi bir kurum, kuruluş, kişi ile mali çıkar çatışması yoktur ve yazarlar arasında çıkar çatışması bulunmamaktadır.