**Huawei'in geçmişle buluşması: Büyük güçler ve telekomünikasyon riski, 1840-2021**

Rush Doshi ve Kevin McGuiness

Brookings Institution, Mart 2021

# Özet

2018 sonlarında, Kanada'nın Huawei'i telekomünikasyon ağlarına kabul edip etmeyeceğine dair Amerika'da endişeler sürerken Kanada Başbakanı Justin Trudeau dünyanın pek çok yerinde kabul gören sağduyuyu yansıtan bir dizi açıklamada bulundu. O zamanlar "Bu, siyasi bir karar olmamalı" diyordu ve Kanada'nın Huawei'in ağlarındaki rolü hakkındaki "kararlarına siyasetin karışmasına izin vermeyeceğini" ifade ediyordu.[1]

Güç diplomasisinin telekomünikasyonla ilgili konulardan ayrı tutulabileceği düşüncesi, yalnızca iyimser değil, aynı zamanda telekomünikasyonun tarihi ile de bağdaşmıyor. Bu raporda, bu geçmişe göz atılarak güç ve telekomünikasyonun nasıl hemen hemen her zaman yakından bağlantılı olduğu gösterilmiştir. Devletlerin bu bağlantıları göz ardı etmesinin ve kendi ağlarının güvenliğiyle fazla övünmelerinin sonuçları dezavantajlı ve zaman zaman felaket boyutunda olmuştur.

Bu raporda, 1840'larda elektrikli telekomünikasyonun ilk ortaya çıktığı zamanlarından itibaren telekomünikasyon alanındaki büyük güç çekişmelerinin başlıca birkaç örneği incelenmiştir. Bu örnekler, günümüzde politikaları hazırlayan kişilerin karşılaştığı birçok sorunun geçmişle yakın benzerlik taşıdığını göstermektedir. Günümüzdeki ağ güvenliği ve 5G altyapısı ile ilgili tartışmalar yeni gibi gelse de bunlar aslında 150 yıl kadar önce elektrikli telekomünikasyonun ortaya çıktığı zamanlardaki unutulmuş tartışmaların birer yansıması. Dahası, standart belirleyici kuruluşlar, devlet sübvansiyonları, kablo başlıkları, bilgi savaşı, gelişmekte olan ülke pazarları ve avantaj elde etmek için şifreleme gibi günümüz telekomünikasyon rekabetindeki bu tanıdık öğeler, yüz yıldan fazla bir süre önce geliştirilmiştir ve günümüzdeki tartışmalar için bunlardan çıkarılabilecek önemli dersler vardır.

Bu önemli derslerin bir listesi aşağıda verilmiştir:

1. **Küresel telekomünikasyon ağlarının kontrolü bir siyasi güç biçimidir.** 5G ağlarının sayısız cihazı ve sensörü birbirine bağlayan daha akıllı, bağlantılı bir ekonominin temellerini oluşturması bekleniyor. Dünya genelinde bu ağları oluşturmaya çok istekli olan Çin, "Dijital İpek Yolu" inisiyatifi kapsamında dünya genelinde 5G lider şirketleri ve projelerine sübvansiyonlar sağlıyor. Bu çaba, Büyük Britanya'nın elektrikli telgrafın ilk zamanlarında ağ hakimiyeti arayışıyla paralellik taşıyor. Britanya, diğer devletlerin Britanya ağlarına bağımlılığını istikrarlı bir şekilde artırarak altmış yıl içinde avantaj elde etti, kablolarını Britanya üzerinden geçirmeye ikna etmek için ücretlerden ve ekonomik avantajlardan dahi fedakarlık ederek aynı zamanda Britanya'nın dış ağlara bağımlılığını da azalttı. Nihayetinde dünyadaki kablo trafiğinin yarısından fazlasının kontrolünü

kazandı, en büyük telsiz ağına ve en büyük kablo gemisi filosuna sahip oldu. Britanya'nın "bilgi hegemonyası", Birinci Dünya Savaşı'nda Almanya'yı hemen hemen tüm küresel telekomünikasyonların dışında bırakmasına olanak sağladı ve Berlin'i trafiğini Britanya takibi riski altındaki hatlara yönlendirmeye zorladı ki bu, Almanya'nın yenilgisinde de belirleyici rol oynadı.

2. **Uzun süren barış ve refah dönemleri genellikle telekomünikasyon riskleri konusunda rehavete yol açar.** Son 30 yıldır, Soğuk Savaş sonrası barış ve ekonomik küreselleşme, telekomünikasyondaki hızlı ilerleme ile birleşince devletler, ağların dış ülkelere ait olması veya dış ülkelerce işletilmesi de dahil olmak üzere, siyasi riskler ve güvenlik risklerinden çok devrimsel ticari avantajlara öncelik verdi. 1840'larda telekomünikasyonun doğuşuyla da benzer bir gelişme yaşandı ve bu da Birinci Dünya Savaşı'na kadar devam eden göreli barış ve küreselleşme dönemiyle beraber ilerledi. Bu çağın büyük kısmında, yeni iletişim teknolojilerinin mucizevi görünen ticari potansiyelini yakalama arzusu, dış ülke ağlarına veya yabancı şirketlere bağımlılıkla ilgili soruları gölgede bıraktı. Büyük Britanya, diğer ülkelerin bu rehavetinden faydalanarak küresel ağlarda mutlak bir kilit konum elde edip bu konumunu kullanırken diğer büyük güçler Britanya ağlarına bağımlı kaldı.

3. **Devletler telekomünikasyon güvenlikleri konusunda rehavete kapıldığında bunun sonuçları felaket boyutunda olabilir ve dünya siyasetini yeniden şekillendirebilir.** Almanların on yıllar boyunca İngiliz telekomünikasyon hatlarına bağımlılığı konusunda rehavetten kurtulamaması sonucunda, Berlin bu bağımlılığın risklerinin farkına vardığında artık durumu değiştirmek için çok geç kalmıştı. Birinci Dünya Savaşı patlak verdiğinde Britanya, Almanya'nın bütün kablolarını kesti ve Berlin'i ele geçirilme riski pahasına trafiğini İngiliz ağları üzerinden yönlendirmeye zorladı. Bu durum sonucunda ele geçirilen "Zimmerman telgrafı", Amerika Birleşik Devletleri'nin savaşa katılmasını sağlamaya yardımcı oldu. Benzer şekilde, Rusların Birinci Dünya Savaşı'nda kablosuz telsiz iletimlerindeki disiplinsizliği Almanların iletişimleri ele geçirmelerine, Rus ordularının hareketlerini gerçek zamanlı olarak "görmelerine" ve Tannenberg Muharebesi'nde Rusları mutlak yenilgiye uğratmasına olanak sağladı. Sonrasında, İkinci Dünya Savaşı'nda Nazilerin şifrelerine aşırı güvenerek güncelleme gereğini hafife alması nedeniyle Büyük Britanya şifreleri kırarak savaşı iki ila dört yıl kısalttığına inanılan istihbaratlar elde etti. Bilginin gücü düşünüldüğünde, en küçük bir muhabere disiplinsizliği ya da rehavet bile tarihi değiştirebilir.

4. **Yeni teknolojiler her zaman yeni ele geçirme çabalarını beraberinde getirir.** Sualtı kablolarının icadıyla bunları kesip kapatma çabaları da İspanyol-Amerikan Savaşı kadar eski tarihlerde görülmeye başlandı; telsiz haberleşmesi, rakiplerin ağ düğümlerini yakalama ve iletişimleri ele geçirme çabalarına yol açtı ve şifreleme için karmaşık şifrelerin ortaya çıkışıyla bunları kırmaya yönelik endüstriyel ölçekte çabalar görülmeye başlandı. Her çağda birileri, telekomünikasyondaki yeni bir açığın öncekiler kadar hassas olmayabileceğine inandı. Ancak her seferinde, inovasyon ve suistimal döngüsü devam etti.

5. **Telekomünikasyon ağları hiçbir zaman siyasi olarak tarafsız olmamıştır, özellikle de ülkeler arası gerginliğin yükseldiği zamanlarda.** 2019'da Huawei yöneticileri "arka kapıdan giriş yok, casusluk yok" yemini etti ve şirketin siyaset dışında kalacağına, Çin hükümetinin bu yemine saygı göstermeyi taahhüt ettiğine dair söz verdi. Fakat yüz yıldan uzun süre önce bile telekomünikasyon şirketleri ve ev sahibi hükümetler kamu önünde benzer sözler verirken bu sözleri gizlice bozuyor ve hem barış hem savaş zamanlarında birlikte çalışıyordu. Örneğin, sualtı kablolarında İngiliz hakimiyeti; Fransız, Alman ve Amerikalıları savaş zamanlarında bile hatları tarafsız tutmayı desteklemeye itti. İngiliz firmaları kamu önünde tarafsızlıklarını ilan ederken esasında, özellikle de tansiyonun iyice yükseldiği anlarda İngiliz siyasi çıkarlarına boyun eğiyor, savaş zamanlarında ise tarafsızlığı hepten bırakıyordu. Rakibin bilgi akışlarını bozma veya ele geçirmenin sağladığı güç, genellikle en samimi tarafsızlık iddialarının bile kalıcılığını bozacak kadar cazip geliyordu.

6. **Devletler bir rakip ya da düşman ülkenin şirketine güvenmenin risklerini fark edince genellikle kendi telekomünikasyon liderlerini yaratmaya çalışır.** Amerika Birleşik Devletleri halihazırda büyük bir 5G baz istasyonu üreticisine sahip değil, bu da kendi şirketlerine mi yatırım yapması yoksa müttefik şirketlere mi güvenmesi gerektiği konusunda tartışmalara yol açıyor. Ayrıca Huawei'in de ne ölçüde fiilen bir devlet destekli lider olduğuna dair tartışmalara da yol açıyor. Bu tartışmaların geçmişte de örnekleri mevcut. 20. yüzyılın başlarında, telekomünikasyon ekipmanı ve ağları için başka ülkelere bağlı bir çok devlet kendi sistemlerini kurmaya başladı. Örneğin, Almanya birbirine rakip telsiz çalışmaları olan iki şirketi (Siemens & Halske ve AEG) İngilizlerin telsiz hakimiyetine bir alternatif kurmak üzere birlikte çalışmaya yönlendirdi. Görünürde özel olan birçok diğer devlet destekli öncü şirket de kendilerini destekleyen devletler ile iç içe geçmiş durumdaydı.

7. **Telekomünikasyon standartları mücadelesi, ağ gücünün hangi devletlerin ellerine geçeceğini belirleyebilir. Bu mücadelede genellikle müttefiklerin ve iş ortaklarının da yardımları gerekir.** Teknolojisi hakim standart olan devletler, diğer ülkelere karşı bu avantajdan yararlanabilir. Bilgi iletişim teknolojisi standartları yarışı şu anki haliyle İngiliz ve Almanların telsiz ağları yarışını andırıyor. Britanya, desteklediği Marconi Company aracılığıyla kablosuz telsiz alanına öylesine hakimdi ki diğer tüm büyük güçler mesajlarını Britanya'nın kablosuz ağı üzerinden geçirmek zorunda kalıyor ve Britanya başka herhangi bir kablosuz istasyonuyla çalışmayı reddediyordu. Almanya, Amerika Birleşik Devletleri ve Fransa dahil diğer güçlerin yardımıyla bu "haberleşmeme" politikasını yasaklayan bir standart belirleyici kuruluş ile bu hakimiyeti kırmayı başardı. Bu, günümüzde de benzer koalisyon yaklaşımlarının liberal devletlerce birlikte çalışmaları halinde avantajlı bilgi ve iletişim teknolojisi (ICT) standartları belirlemek veya sürdürmek için nasıl kullanılabileceğini gösteren bir örnek.

8. **Devletler, iletişimlerini ele geçirmek kolaylaştıkça şifrelemeye yönelir ancak şifreleme de kararlı düşmanlar veya kullanıcı hataları nedeniyle sınırlı kalır.** Kimileri Huawei'in ağlardaki rolüne ilişkin endişelerin veya internete bağlı cihazların genel olarak riske açık olma durumunun modern şifreleme ile hafiflediğini savunur. Bu tür argümanların uzun bir geçmişi vardır. Yüz yıl önce telekomünikasyonun ilk

zamanlarında, telgraf mesajlarının ağ düğümlerini kontrol edenlerce okunabilme veya telsiz iletişiminin pasif dinleme ekipmanlarıyla ele geçirilme ihtimali büyük şifreleme girişimlerine yol açmış ve bu da genellikle aşırı güveni beraberinde getirmiştir. Almanya'nın karmaşık rotor şifre makinelerinin kırılamaz olduğuna inanılıyordu ancak kullanıcı hatası ve Britanya'nın endüstriyel ölçekteki çabaları, Büyük Britanya'nın Alman kodlarını tehlikeye atmasına olanak sağladı. Alman ekipman ve şifrelerinde düşük maliyetli güncellemeler Britanya'nın avantajına son verebilecekken Berlin'in şifreleme sistemine aşırı güvenmesi bu değişikliklerin önüne geçerek savaşın şeklini değiştiren istihbarat sızıntısına neden oldu. Uçtan uca şifreleme önceki şifreleme çabalarına göre büyük ölçüde daha gelişmiş olsa da tarihe bakıldığında biraz mütevazı olmanın faydalı olacağı anlaşılıyor.

9. **Birçok devlet, iletişim ağlarını ele geçirmek için düşmanlarının ne derecede çaba gösterebileceğini genellikle hafife alır.** Modern telekomünikasyonla ilgili tartışmalar sürerken, rahatlığa veya ticarete öncelik veren ve bu nedenle güvenlik konusunda kestirmelere başvuran devletlerin, kararlı bir düşmanın ağlarını tehlikeye atmak için göstereceği çabayla olumsuz bir sürpriz yaşama ihtimalinin yüksek olduğunu hatırlatmakta yarar var. Birinci Dünya Savaşı'nda Almanya, dış dünyaya erişmek için kullandığı tüm kabloların Britanya tarafından ne kadar hızlı ve acımasız bir şekilde kesildiğini görünce şaşkınlığa uğramıştı; benzer şekilde Rus komutanlar da telsiz disiplinsizlikleri nedeniyle Tannenberg'de felaket bir yenilgiye uğradıklarında çok şaşırmıştı. İkinci Dünya Savaşı'nda Almanya, İngilizlerin Alman kodlarını kırmak amacıyla çok küçük ya da anlık da olsa Almanya'nın iletişim hatalarından faydalanmak için yüksek oranda merkezileştirilmiş, endüstriyel ölçekte bir şifre kırma operasyonu kurmasını beklemiyordu. Soğuk Savaş döneminde Sovyetler, Amerika Birleşik Devletleri'nin erişimi dışında olduğunu düşündükleri için hiçbir ülke içi sualtı telefon hattını şifrelemedi fakat Washington bu hatlara kablo başlığı takmanın bir yolunu bularak paha biçilemez bir istihbarat kaynağı elde etti.

10. **Ağ güvenliği yalnızca ele geçirmeyi değil hizmet dışı bırakmayı da kapsar.** Huawei'in ağlardaki rolüne ilişkin bazı tartışmalarda veri güvenliği sorunu vurgulanıyor ancak büyük güçlerin telekomünikasyon yarışının önemli bir parçası olan ağları hizmet dışı bırakmayı da bu tartışmalara dahil etmekte yarar var. Telgrafın ilk zamanlarında büyük güçler, kabloları kesip iletişimi devre dışı bırakmaya çalışıyordu. Bunun en uç noktası, Büyük Britanya'nın Almanya'yı dış dünyaya bağlayabilecek bütün kabloları etkisiz hale getirmeye yönelik eşi benzeri görülmemiş ve en ince ayrıntısına kadar planlanmış operasyonuydu. Bazen devletler ağları hizmet dışı bırakma stratejileriyle kendilerine zarar verse de rakibinin daha fazla zarar gördüğüne inanması halinde bundan geri durmaz.

## Büyük güçler ve telekomünikasyon

Bir telekomünikasyon tarihi anlatımında şöyle deniyor: "Büyük imparatorluklar, bilgi akışını hızlandırmak için her yola başvurdu". "Romalılar yollar inşa etti, Persler ve Moğollar atlarla bilgi taşıma ağları kurdu, İngilizler posta vapurlarına finansal destek sağladı."[2] Ancak devletler bilgi için yanıp tutuşsa da modern telgrafın doğuşuna kadar bilgi akışı sınırlı kaldı. Bilgi akışlarının elektrikli hale getirilmesiyle birlikte modern telekomünikasyon ortaya çıktı ve bunun sonucunda da büyük güçlerin bilindik rekabet modelleri oluştu.

1840'lardan Birinci Dünya Savaşı'na kadar olan modern telekomünikasyonun ilk on yılları günümüzle benzer karakteristik özellikler taşıyor. Mevcut Soğuk Savaş sonrası dönem gibi bu dönem de lider devletlerin telekomünikasyon ağlarında siyaset ve güvenlik meselelerine karşı "daha az hassas"[3] olmasına neden olan, büyük güçlerin görece barış içinde olduğu bir dönemdi. 19. yüzyılda büyük güçler ulusal ve uluslararası ağlar oluşturdukça çoğu başlangıçta her şeyi endüstriye bırakmaktan, özel şirketlerin ulusallığını göz ardı etmekten ve telekomünikasyon ağlarının kontrolünün bir düşmanın eline geçmesinin risklerini önemsiz görmekten memnundu. O dönemde kimilerince "zamanın ve mekanın yok oluşu" olarak adlandırılan telekomünikasyondaki devrimsel değişimlerin avantajları[4] öylesine bariz ve karşı konulmazdı ki "kabloların mülkiyeti görece küçük bir sorundu".[5] Telgraf o dönemde siyasetten çok işle ilgiliydi, diyor bir tarihçi. Bu gözlem, modern bilişim teknolojisi ve onun son ürünü olan 5G'ye yönelik en başta duyulan heyecan için de aynı şekilde geçerli görünüyor .[6]

Büyük güçlerin görece rehavette olduğu dönem fazla uzun sürmedi. 1879'da Peru gibi ülkeler ve 1898'de Amerika Birleşik Devletleri, rakiplerinin telekomünikasyon ağlarını kesen ilk devletlerden bazılarıydı. Büyük güçler arasındaki gerilim arttıkça dünya genelinde devletler uyanarak bazılarının (Büyük Britanya) uzun barış dönemini iyi yönettiğini ve özel şirketleri aracılığıyla uluslararası iletişimlerde mutlak güç elde ettiğini fark etti.

Britanya'nın sualtı kablo ağlarına bağımlı olmaktan giderek daha fazla korkan Fransa ve Almanya gibi devletler kendi ağlarını geliştirmek için büyük oranda finansal destek sağladı. Bu, Çin'in sübvansiyonlarından ve Alibaba, Baidu, Tencent ve Huawei gibi bilişim teknolojisi liderlerini korumasından pek de farklı değil. Tarihçi Heidi Tworek'in belgelediği gibi, Britanya'nın rakipleri Britanya'ya ait sualtı telgraf kablolarına bağımlılığı azaltma umuduyla telekomünikasyon teknolojisinin bir sonraki nesli ("telsiz telgraf", yani bilinen adıyla telsiz) üzerine büyük yatırımlarda bulundu.[7] Britanya bu alandaki liderliğini korurken Almanya, İngiliz ağlarına güvenmeyi reddetti. Bugün Çinli teknoloji şirketlerinin gelişen dünyaya açılmasına ve Pekin'in 5G ağlarının temellerini atma kararlılığına benzer şekilde Almanya; Latin Amerika, Afrika, Asya gibi dünyanın daha az bağlantılı kısımlarına yatırım yaparak devlet destekli lider şirketlerle kendi ağlarını oluşturdu.

Bu dönem boyunca, büyük güçlerin telekomünikasyon rekabetinin günümüzde gözden kaçırılan birçok öğesi, o çağın devletleri tarafından genellikle oldukça ciddiye alınıyordu. Telsiz ağlarında İngiliz hakimiyetinden rahatsızlık duyan Almanya, İngiliz hakimiyetini kırmak için bir standart belirleyici kuruluş kullandı. Bu durum, bu kuruluşların o dönemde de en az bugünkü kadar önemli olduğunu gösteriyor. Telekomünikasyon kablosuza kaydıkça ve ele geçirmesi daha da kolaylaştıkça, büyük güçler şifrelemeden medet umarak, ağlarının disiplinli bir şekilde

işletilmesini terk ederek mesajları şifrelemek ve şifrelerini çözmeye yönelik ayrıntılı adımlar olan "şifrelerin" sorunu çözeceğini varsaymış ancak bu, kullanıcı hatası nedeniyle hemen hemen her zaman yanıltıcı olmuştur. Bu görüş, telekomünikasyon ağlarının genel güvensizliğine ilişkin modern varsayımlarla ve bazı tartışmalarda dile getirilen Huawei şifrelemesinin Çin'in telekomünikasyon ağlarını ele geçirme riskini büyük ölçüde etkisiz hale getirebileceği görüşüyle çarpıcı benzerlikler taşıyor.

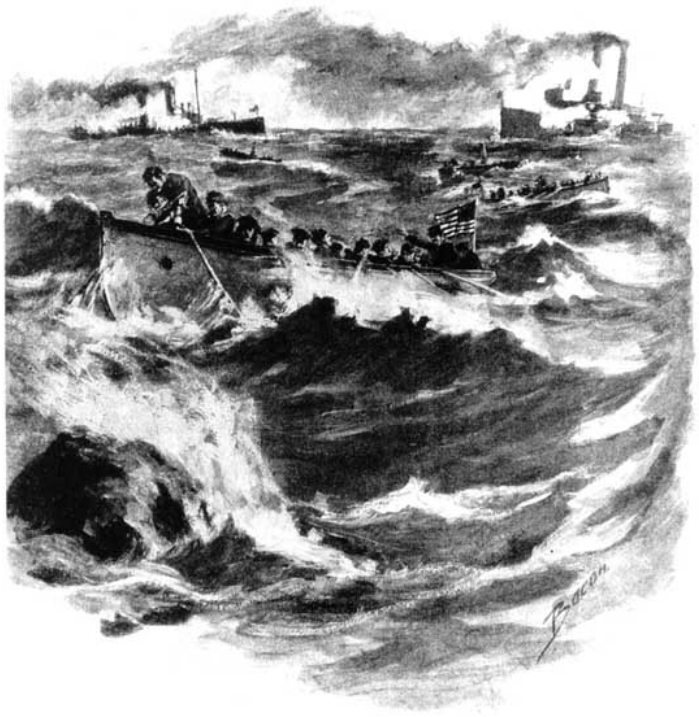
Büyük güçlerin barışı sona erip savaş patlak verdiğinde, barış zamanlarında her zaman belirgin olmayan telekomünikasyonun önemi birden bariz hale geldi. Almanların Birinci Dünya Savaşı'nda Rus iletişimlerini ele geçirme başarısı, Tannenberg Muharebesi'nde öylesine büyük bir zafer getirdi ki savaşın seyri değişti ve Rusya'nın çatışmadan çekilmesi hızlandırılmış oldu. Birinci Dünya Savaşı'nda İngilizlerin sualtı kablolarına tamamen hakim olması, Almanları küresel telekomünikasyon sisteminden kopartarak Alman kablo trafiğini İngiliz ağları üzerinden yönlendirmeye itti ve bunun sonucunda, Amerika Birleşik Devletleri'nin çatışmaya girmesine yardımcı olan Zimmerman telgrafı ele geçirildi. İkinci Dünya Savaşı'nda Britanya, Almanların kırılamaz denen şifrelemesini kırarak Britanya resmi tarihinde Avrupa'daki savaşı birkaç yıl kısalttığı söylenen benzersiz bir istihbarat elde etti. Bu örnekler telekomünikasyon güvenliğinin yalnızca bir muharebe alanı taktiği değil, siyasi rekabet konusu olduğunu, büyük güçlerin kaderini belirleyebilecek ve dünya tarihinin akışını değiştirebilecek öneme sahip olduğunu gösteriyor.

Dünya, ABD ile Sovyetler Birliği arasındaki Soğuk Savaş'a doğru giderken hem Amerika'nın gücü hem de eski ağların önemini azaltan teknoloji atılımları nedeniyle Britanya'nın avantajları kayboldu. Bu da büyük güçlerin teknolojinin ön saflarında kalmasının önemini gözler önüne seriyor. Bu yeni çağda, telekomünikasyon yarışı benzer hatlar üzerinden devam etti. Örneğin, Amerika Birleşik Devletleri çok derine gömülmüş olan ve çok güvenli olduğu düşünüldüğü için buralardan aktarılan mesajların genellikle şifrelenmeden bırakıldığı sualtı kablolarına kablo başlığı takmanın yeni yollarını bulmada öncü rol oynadı. Rekabet, uydu ve internet altyapısı gibi diğer alanlara da taşındı ancak bu alandaki tarih hâlâ yazılmaya devam ediyor ve çoğu durumda bu bilgiler gizli bilgi kapsamına giriyor.

Bu kısa örnekler dizisinde de görüldüğü gibi, telekomünikasyon her zaman siyasi olagelmiştir. Bu teknolojilerin ve yetkinliklerin suistimal edilmesi, genellikle teknolojilerin gelişimleriyle birlikte evrimleşmiştir. Yeni iletişim yöntemleri ortaya çıkar çıkmaz büyük güçler genellikle bunları ele geçirmenin ya da engellemenin yollarını aramıştır. Bir telekomünikasyon tarihçisi "Elektrikli iletişimler genellikle insanlığın en büyük başarılarından biri olarak tanımlanır ancak güvenlik açısından baktığımızda tamamen farklı bir durum görürüz çünkü güvenlik teknik değil, sosyal ve siyasi bir özelliktir" diyor. "Siyaset gelişmediği için de telekomünikasyonu karanlık bir tarafı vardır" diye de ekliyor.[8]

Şimdi de telekomünikasyon yarışının yaklaşık iki yüz yıllık tarihi boyunca görülen başlıca temaların bir özetini ele alacağız.

# 1. İspanyol-Amerikan Savaşı: Kablo tarafsızlığının sınırları



*1907'de yayımlanan ABD'nin Cienfuegos'da kablo kesme seferinin bir betimlemesi. Bu operasyon, bir zamanlar kablo tarafsızlığını savunan bir büyük güç için bile silahlı çatışma zamanlarında sualtı telgraf kablolarına tarafsız muamele edilemeyeceğini göstermiştir.*

*Kaynak: Naval Historical Center Çevrimiçi Kütüphanesi*[9]

19. yüzyılda sualtı kabloları dünyayı çevrelemeye başladığında, Fransa, Almanya ve Amerika Birleşik Devletleri dahil birçok lider güç bunların uluslararası siyasetten ayrı tutulmasını talep etti. 1858'de, dünyanın ilk transatlantik kabloları gönderilirken ABD Başkanı James Buchanan, Kraliçe Victoria'dan yeni telgraf hatlarının "silahlı çatışma zamanlarında bile... her zaman tarafsız" kalması yönünde davranmasını istedi.[10]

Silahlı çatışmalar ortaya çıktığında ise yüce gönüllü tarafsızlık ilkeleri terk edildi. Buchanan'ın mesajından yirmi yıl sonra Peru, tartışmalı topraklara giren Şili kablo hatlarını kesti.[11] Bu anlaşmazlık pek fazla dikkat çekmedi ancak bir zamanlar kablo tarafsızlığını savunan Amerika Birleşik Devletleri, İspanyol-Amerikan Savaşı'nda hem Atlantik'teki hem de Pasifik'teki kabloları kesince dünya dikkat kesildi.

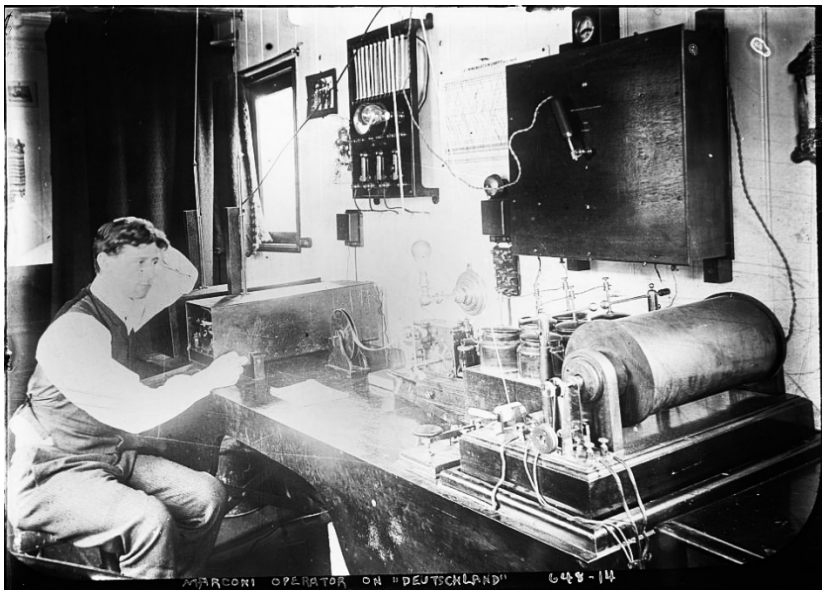
Amerika'nın kabloları kesmesi, çatışmadan önce planlanmıştı. Atlantik harekat alanında Amerika Birleşik Devletleri, İspanya'nın Küba'daki kuvvetleriyle bağlantısını kesmeyi umuyordu. O tarihte yayınlanan bir Amerikan dergisi "Havana'nın izole edilmesi elbette çok önemliydi" diye yazdı ve Amerika Birleşik Devletleri'nin "Havana'nın dış dünyayla tüm telgraf iletişimini kesmesi" gerektiğini ifade etti.[12] Amerika Birleşik Devletleri, Florida'da Amerikan topraklarından geçen İspanyol trafiğini kesmekle işe başladı. Ardından küçük bir Amerikan

ekibini Cienfuegos'daki önemli bir telekomünikasyon ağı düğümünü imha etmekle görevlendirerek Havana şehrinin ve batı Küba'nın büyük bir kısmının İspanya'yla bağlantısını kesti. Sonrasında, Amerika Birleşik Devletleri doğu Küba'daki pek çok kablonun yanı sıra Porto Riko ile İspanya'yı birbirine bağlayan Karayip kablolarına da saldırdı.[13] Bu kablo kesme operasyonları, İspanya'nın Küba'daki kuvvetleri yönetme ve kumanda etme kabiliyetini önemli ölçüde zayıflattı.[14]

Pasifik'te, Amerika Birleşik Devletleri Manila ile Hong Kong arasındaki tek sualtı kablosunu keserek Filipinler'in İspanya'yla bağlantısını etkili bir şekilde kopardı.[15] Bu karar ABD iletişimlerine de zarar verdi ancak İspanyollara daha da fazla zarar verdiği düşünülüyordu ve Amerika Birleşik Devletleri, Hong Kong'a düzenli olarak bir gemi göndererek oradan gelen mesajları Washington'a taşıtıyordu.[16] ABD kuvvetleri, Filipinler'deki sualtı kablolarını da keserek İspanya'nın kuvvetlerine komuta etme kabiliyetine bir zarar daha verdi.

İspanyol-Amerikan Savaşı belki de elektrikli telekomünikasyonun önemli olduğu birden fazla harekat alanına yayılan ilk küresel çatışmaydı. Ayrıca bir büyük gücün bir diğerinin sualtı kablolarına erişimini engellemeye çalıştığı ilk örnekti. Çatışmadan önce telgraf hâlâ birincil olarak ticari bir alan olarak görülüyor ve birçoğu, kabloların siyasi ve askeri mücadeleden korunabileceğini umuyordu. Bu çatışma, bu bakış açılarının sınırlı olduğunu kanıtlayarak telekomünikasyon altyapısının kontrolünün ve jeopolitik rakiplere bu avantajların verilmemesinin her zaman için kritik bir siyasi öneme sahip olduğunu gösterdi.

## 2. İngiliz-Alman rekabeti: Ağlar inşa etme ve standartları belirleme




*Marconi Company telsiz operatörü, Alman okyanus gemisi SS Deutschland'ın "Marconi Odası"nda. Marconi Company'nin etkisi o kadar güçlüydü ki Almanya'nın ele geçirme ve hizmet reddi risklerine dair endişelerine rağmen Alman telsiz odalarında şirket çalışanları görevlendiriliyordu.*

*Kaynak: Library of Congress, George Grantham Bain Collection [Kongre Kütüphanesi, George Grantham Bain Koleksiyonu]*[17]

Teknolojik standartları belirleme ve bunun ağ üzerindeki etkileri, büyük güç mücadelesinin eskiden beri var olan, incelikli bir arenasıdır. Teknolojisi hakim standart olan devletler, diğer ülkelere karşı bu avantajdan yararlanabilir. Paralel sistemler yaratarak hassasiyetlerini azaltmaya çalışan yükselen güçler için de bu nokta gözden kaçmaz. Aslında günümüzdeki Çin ile Amerika arasında görülen ICT yarışı, Almanya ile Büyük Britanya arasında o çağın ICT altyapısına hakim olma yarışına benziyor. Durumu incelediğimizde iki olayın ne büyük benzerlikler paylaştığını fark edebilir ve günümüz için önemli dersler çıkarabiliriz.

19. yüzyıl sonlarında, İtalyan mühendis Guglielmo Marconi İngiliz Kraliyet Donanması'nın desteğiyle telsiz telgrafı icat etti.[18] Bu buluş devrim niteliğindeydi. Geçmişte büyük güçler birbirlerinin kablolarını kesmişken ve gemiden gemiye ve gemiden karaya iletişimlerde zorluklar yaşanmışken Marconi'nin sistemi bu sorunlara bir çözüm getiriyordu ve müdahalelere karşı daha güçlüydü.[19] Marconi daha sonra Büyük Britanya ile ortaklık kurarak ülkeye telsiz iletişimleri alanında tekellik kazandırdı. Britanya'nın dünya sualtı kablo ağının %60'ına da sahip olması neticesinde Britanya, uluslararası iletimlere hakim konuma geldi. İngilizlerin bu avantajı Almanya'yı rahatsız etse de kablosuz teknolojilere yönelik yarış "Almanya için yeni bir uluslararası altyapının kontrolünü elde etme" ve "Britanya'nın kablolarından kurtulma" fırsatı da sunuyordu ve bunun sonucunda büyük bir güç üstünlüğü elde etme şansı vardı.[20]

Kendini savunmasız hisseden Alman İmparatoru II. Wilhelm, Marconi'nin tasarımlarını başarılı bir şekilde kopyalayan, Almanya içinde bunların patentini alan ve Alman ordusuyla yapılan sözleşmelerle finanse edilen kendi telsiz ağlarını kuran Alman bilim insanlarına ve mühendislere doğrudan devlet desteği verme yetkisi çıkardı.[21] Buna rağmen, Marconi'nin üstün uzun menzilli telsizi ve ilk harekete geçen olma avantajı, Britanya destekli şirketinin küresel standart olmasını sağladı ve Marconi, bu ağ etkilerinden faydalanarak Marconi telsizi dışı operatörlerle "haberleşmeme" politikası izledi. Alman işletmeleri ve okyanus gemileri küresel iletişimden kopmak istemediği için Britanya destekli sistemi Alman sistemine tercih ettiler.

Alman İmparatoru II. Wilhelm, İngiliz standardına meydan okumak için Alman endüstriyel politikasını güçlendirdi. Telsiz çalışmalarında birbirine rakip iki büyük Alman elektrik şirketi olan Siemens & Halske ve AEG'nin mutlak Alman alternatifi Telefunken'i kurmak üzere birleşmesi için bir kararname yayımladı. İmparatora göre "Telsiz telgraf alanındaki [yurt içi] rekabet, Almanya'nın rekabet gücünü zayıflatıyor" ve "Marconi Company'ye Almanya'nın menfaatine uygun olmayan bir şekilde dünya genelinde tekel olma fırsatı veriyordu".[22] İmparator II. Wilhelm yönetiminde Almanya bazı durumlarda Marconi sistemlerini yasaklayarak korumacılık politikası izledi. Güney Amerika ve Afrika'ya kendi teknolojisini satarak bu bölgelerde kendi standartlarını belirlemek ve geliri güvence altına almak amacıyla gelişmekte olan pazarlara yöneldi.

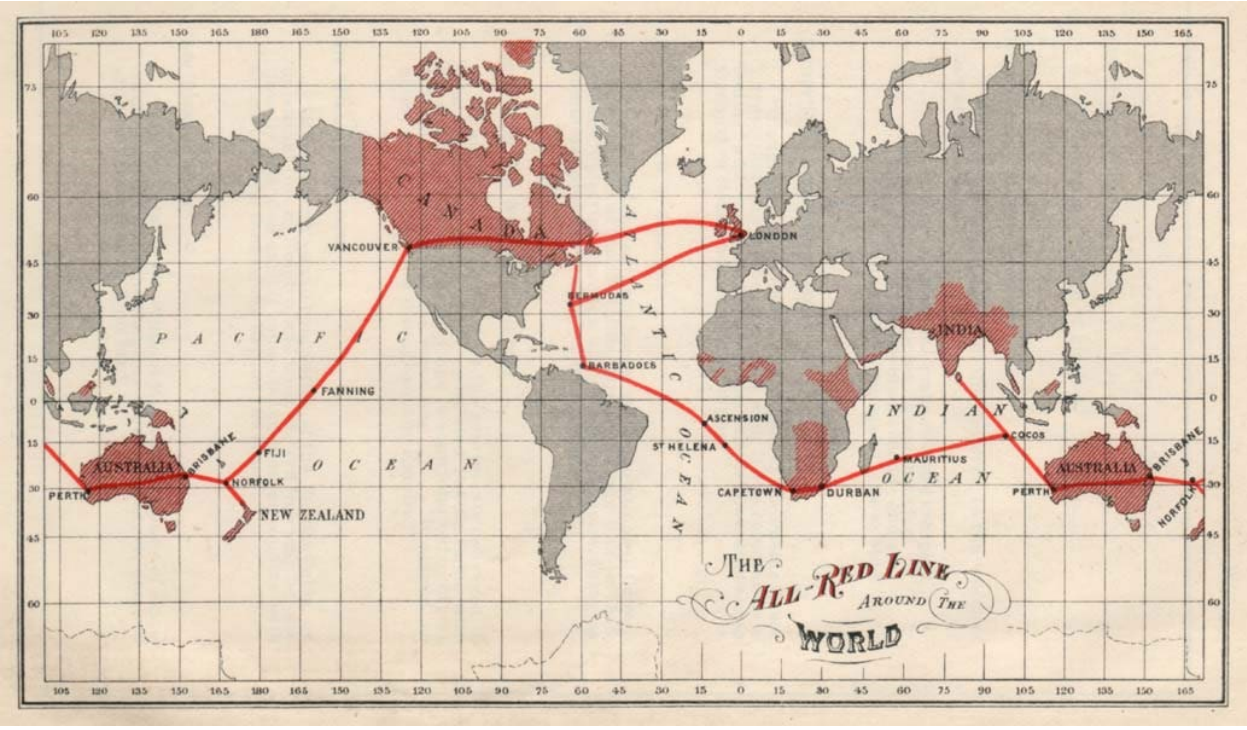
Bu çabalar yetersiz kalınca Almanya çözümü çok taraflı standart belirleyici kuruluşlarda buldu. 1906'da Almanya, telsiz standartları üzerine bir konferans olan dünyanın ilk Uluslararası Telsiz Telgraf Konvansiyonu'nda büyük güçleri bir araya topladı. Burada, üyeler Marconi'nin "haberleşmeme" politikasını ortaklaşa yasaklayarak İngiliz tekelini kırdı ve etkili bir İngiliz-Alman duopolisi kurdu.[23]

İngiliz-Alman rekabeti, standart belirleyici kuruluşların çok büyük stratejik etkileri olduğunu ortaya koyuyor. Çin bugün Almanya'nın yüz yıl önce kullandığı tekniklerin birçoğunu kullanıyor. Devlet yönetiminde endüstriyel politika, devlet koruması, bol kaynaklı devlet sözleşmeleri, sivil-askeri entegrasyonu, rakip ürün yasakları, zorla şirket birleşmeleri, gelişmekte olan pazarlara yönelme ve hatta kendi standartlarını belirlemek için uluslararası antlaşmalar gibi yöntemlerin tümü, WeChat ve AliPay'in sahipleri Alibaba ve Tencent gibi Çinli teknoloji şirketlerinin yerel liderler olmasına yardımcı oldu. Bu şirketler yurt dışına açılarak ABD pazarlarını değil, kendilerinden önce Almanya'nın Telefunken şirketinin yaptığı gibi daha düşük kâr ve daha az rekabetin olduğu gelişmekte olan pazarları hedef aldı.[24]

Çin, internet bağlantısının fiziki altyapısı alanında da standart yarışını bırakmıyor. Çinli çip üreticilerinin 5G mobil internet standartları yarışında Amerikan rakiplerini yenebilmesi için hükümet milyarlar değerinde yatırım yapıyor. Benzer şekilde, Huawei ve ZTE gibi Çinli şirketler gelişmekte olan dünyada internet bağlantısının fiziki altyapısını kurmak üzere devlet kredileri alıyor. Britanya örneğinde görüldüğü gibi, bu çabalar yalnızca Çin teknolojisini standart hale getirmekle kalmıyor, aynı zamanda gözetim fırsatları da sunuyor. Diğer taraftan, Bir Kuşak Bir Yol İnisiyatifi, Asya genelinde özellikle de ilgili sensör ve yazılımlarda "akıllı altyapı" standartlarının Çin tarafından belirlenme ihtimalini ve diğer şirketlerle birlikte çalışmanın kabul edilmeyerek bunların otonom araç endüstrisi ve diğer endüstrilerden dışlanabileceği ihtimalini doğuruyor.

İngiliz ve Almanların telgraftaki rekabeti, Washington'ın Çin'in standartlarda devlet yönetiminde meydan okumasını ciddiye alması gerektiğini gösteriyor. Aynı zamanda bir çıkış yolu da sunuyor. Almanya'nın telgraf alanında İngiliz tekelini kırmak için uluslararası konferansları kullandığı gibi, Amerika Birleşik Devletleri de çok taraflı anlaşmalar aracılığıyla avantajlı ICT standartları belirleyebilir veya sürdürebilir. Bunu yaparak Çin'in serbest ticaret anlaşmaları, devlet destekli lider şirketler veya altyapı projeleri aracılığıyla tek taraflı standart belirlemesinin önüne geçebilir.

## 3. Birinci Dünya Savaşı'nda Britanya: Bilgi hegemonyasını kullanma




*"All Red Line", devasa bir yedeklilik ile kurulan ve hiçbir kısmı bir rakibin topraklarından geçmeyecek şekilde düzenlenen Britanya'nın maliyetli sualtı kablo ağı. Almanya'nın kendi esnek küresel iletişim ağı yatırımının yetersiz olması, Britanya'nın Almanya'nın küresel iletişim ağıyla bağlantısını kesmesini sağlarken Britanya genel olarak etkilenmeden kaldı.*

*Kaynak: George Johnson, ed.,* All Red Line: The Annals and Aims of the Pacific Cable Project [All Red Line: Pasifik Kablo Projesinin Tarihi ve Amaçları] / İnternet Arşivi[25]

Almanya'nın 20. yüzyıl başlarında telekomünikasyonda İngiliz hakimiyetini kırma çabaları paranoyadan kaynaklanmıyordu. Birinci Dünya Savaşı çıktığında Britanya telekomünikasyon ağlarındaki ciddi etkisini savaşın gidişatını şekillendirmek için başarıyla kullandı. Almanya'nın kablolarını kesti, Almanya'nın ilettiği mesajları takip etti ve Alman trafiğini Britanya kontrolündeki ağlar üzerinden yönlendirmeye zorlayarak Amerika'nın savaşa katılmasını sağlamaya yardımcı olan Zimmerman telgrafını ele geçirdi.[26]

Büyük Britanya, telekomünikasyon ağlarını kesen ya da manipüle eden ilk büyük güç değildi. Peru Şili-Bolivya bağlantısını kesmiş, Amerika Birleşik Devletleri İspanyol kablolarını kesmiş ve Britanya bir kriz sırasında Boer'lerin Avrupalı destekçileri ile bağlantısını keserken bir diğer krizde ise Fransa'ya giden kablo trafiğini manipüle etmişti.[27] Fakat Birinci Dünya Savaşı'nda bu tarz müdahaleler uç noktaya taşındı.

Büyük Britanya, tüm bir ülkeyi ana akım küresel telekomünikasyon ağından tamamen kopartarak barış zamanlarında dikkatlice düşünülmüş bir planı savaşın birinci gününden uygulamaya koyan ilk ülkeydi.[28] Bir yıl içinde Büyük Britanya dünyanın her yerindeki Alman kablolarına zarar

verdi: İngiliz Kanalı, Kuzey Denizi, Kuzey Atlantik, Güney Amerika, Afrika'nın çoğunluğu, Uzak Doğu ve hatta Alman altyapılarını barındıran tarafsız ülkelerde bile.[29]

Bunu telafi etmek için Almanya, Telefunken'in bir ay önce Latin Amerika'da ve "Küresel Güney"de kurduğu telsiz ağlarını dünyayı kapsayacak şekilde genişletmeye çalıştı. Çin'in Dijital İpek Yolu ile modern paralellik gösteren bir çabayla Berlin, "telsizin gelişimsel avantajları" ile ilgilenen hükümetlere Alman telekomünikasyon ağı düğümlerini barındırmaları için kredi ve yatırım tekliflerinde bulundu. Buna karşılık, Büyük Britanya bu ülkelerin çoğunu Alman telsiz ağı düğümlerine destek vermekten vazgeçmeye ikna veya teşvik etti ya da eyleme geçerek bu düğümleri sabote etti.[30]

Kendine ait ağları olmayan Berlin'in savaş sırasında Britanya'nın ağlarına güvenmekten başka seçeneği kalmadı. Başlangıçta İngilizler kendi kablolarından geçen tüm trafiği sessizle izlemeyle başladılar ve bu avantajı Almanya'ya bilgi savaşı açmak için kullanarak Almanya'nın tarafsız ülkelerle ilişkilerine zarar vermek için küçük düşürücü Alman trafiklerini seçerek bu bilgileri sızdırdılar. Almanya, Amerika Birleşik Devletleri'ne karşı Meksika ile bir askeri ittifak önerisi içeren bir telgraf (meşhur Zimmerman telgrafı) gönderince bu mesaj bir İngiliz ağından geçerken Büyük Britanya tarafından ele geçirilerek şifresi çözüldü. Ardından Britanya bu telgrafı Amerika Birleşik Devletleri ile paylaştı ve Amerika da bunu kamuoyuna sundu.[31] Bu olay, Amerika Birleşik Devletleri'ni savaşa sokmaya yardımcı olarak dünya tarihini şekillendirdi ve Almanya'nın mağlubiyetine zemin hazırladı.

İngilizlerin Almanya'ya açtığı bilgi savaşı, bir rakip güce trafiğini izleme imkanı vermenin veya telekomünikasyon erişiminin kesilmesinin tehlikelerini gözler önüne seriyor. Ayrıca, büyük güçlerin barış zamanlarında varlığını kanıksadığı ağların savaş zamanlarında engellenebileceğini ve iletişim ağı düğümleri mücadelesinin kaçınılmaz olarak üçüncü tarafları ve tarafsız ülkeleri de içereceğini gösteriyor.

# 4. Almanya'nın Tannenberg zaferi: Ele geçirmenin tehlikeleri


*Birinci Dünya Savaşı sırasında bir Alman kablosuz saha telgraf istasyonu. Rusya'nın, saha istasyonlarındaki iletişimlerini yeterli şekilde şifreleyememesi savaşın gidişatını değiştiren felaket bir yenilgi ile sonuçlandı.*

*Kaynak: C. O. Nordensvan ve Valdemar Langlet,* Det stora världskriget *[Büyük Dünya Savaşı]*[32]

Almanya bilgi savaşında kendi imkanlarından tamamen yoksun değildi. Rusya'nın Batılı müttefikleri ile bağlantısını sağlayan çok sayıda kara ve sualtı kablosunu ve ayrıca İngilizlerin güvendiği birçok transatlantik kablosunu keserek bu görevler için denizaltıların kullanımına öncülük etti.[33] Britanya ağlarının yedekliliği düşünüldüğünde bu çabalar Almanların umduğu kadar zayıflatıcı bir etki yaratmadı. Çok daha fazla sonuç getiren bir adım ise Almanya'nın Ağustos 1914'te, savaşın ilk ayında, Tannenberg Muharebesi'nde Rusya'ya karşı telsiz istihbaratını kullanarak Rusları mutlak bir yenilgiye götürmesi oldu. Bir Alman istihbarat subayı o dönemde bu olayı "düşmanın telsiz trafiğinin ele geçirilmesinin belirleyici bir rol oynadığı insanlık tarihindeki ilk an" olarak yorumladı.[34]

Muharebe, Rusların Doğu cephesinde kazanımlar elde ettiği bir anda gerçekleşti. Rusya, Doğu Prusya'ya doğru ilerledikçe ordusu ciddi bir iletişim zorluğuyla karşılaştı ve bu durum felaket bir yenilgiye zemin hazırladı. Geri çekilen Almanlar kendi telgraf hatlarını kesmişti ve ilerleyen Ruslar, yayıldıkları alanlarda kablolu iletişim ağları kurabilecek yeterli eğitimli personele sahip değildi. Telsiz iletişimi bir alternatif olarak kullanıldı ancak Ruslar askeri komuta ve kontrol için yeni telsiz teknolojileri kullanmaya başlamışlar ve bunu yeterince güvenli hale getirmemişlerdi. Farklı şifrelere farklı gruplar atanmıştı ve birçoğu haberleşmeleri şifreleme ve şifrelerini çözme konusunda çok az eğitim almıştı; bazı kodların İngilizlerce kırıldığı biliniyordu ve sınırlı sayıdaki kod kitaplarını çoğu okuma yazma bilmeyen askerler okuyamıyordu.[35] Bunun sonucunda Rus komutanlar kodlanmamış telsiz mesajları kullanma riskini göze almak zorunda olduklarını düşündü ve Almanların kendilerini çok dikkatli bir şekilde izliyor olmadığını umdu.

Ancak Almanlar haberleşmeleri çok yakından takip ediyordu. Rusların Japonlarla savaşta telsiz disiplinsizliğini gözlemledikten sonra kodlanmamış iletimlerin bir aldatma kampanyası

olmadığını biliyorlardı. Bu nedenle, Rus iletişimleri hakkındaki gerçek zamanlı bilgilerini "savaşın sisini" dağıtmak ve üstün gücü kesin olarak mağlup etmek için kullandılar. Rusya tüm ordusunu kaybetti, 100.000'den fazla asker hayatını kaybederken 92.000 asker esir alındı; Almanya'nın can kaybı ise yalnızca 13.000 askerdi.

# 5. İkinci Dünya Savaşı'nda Britanya: Şifrelemenin sınırları

*İkinci Dünya Savaşı sırasında etkin olarak kırılamaz olduğu düşünülen Lorenz şifreleme makinesinin mekanik rotorları. İngilizlerin şifre kırma çabaları, subayların üst düzey Alman iletişimlerine erişmesini sağladı.*

*Kaynak: Matt Crypto / Wikimedia Commons*[36]

Telsiz telgraf ve telsizin icat edilmesi fiziksel kablolara göre daha fazla rahatlık sağlamakla birlikte daha fazla ele geçirilme riski taşıyordu. Birinci ve İkinci Dünya Savaşları'nda, büyük güçler telsiz iletişimlerinin diğerleri tarafından erişilebilir olduğunun varsayıldığı bir dünyada yaşıyordu. Modern bilgisayar ve telekomünikasyon sistemlerinin hassasiyetine dair mevcut varsayımlardan pek de farklı olmayan böyle bir dünyada şifreleme, güvenlik açısından kritik addediliyordu. Bunun sonucu, bir Amerikan askeri tarihçisinin ifade ettiği gibi "kriptograf ve kripto analiz uzmanları arasında bir mücadele" oldu.[37] Büyük güçler, mücadelenin yanlış tarafında yer aldığında bunun sonuçları felaket boyutunda olabiliyordu.

Böylesi bir sonucu önlemek için kuruluşlar ele geçirmenin güvenliği tehlikeye atma riskini azaltacak şifreler kullanıyordu. Ayrıca düşmanların telsiz trafiği analizi aracılığıyla kullanım düzenleri hakkında fikir edinmelerini engellemek için "telsiz disiplini" uyguluyordu.

Birçok büyük güç, düşman trafiğini incelemek ve mümkünse düşman şifrelerini kırmak için gerçek anlamda endüstriyel bir çaba sarf ediyordu. Büyük Britanya düşman şifrelerini analiz etmede Almanya'ya göre çok daha merkezileşmiş, Almanya ise bu işlevleri birkaç organa dağıtmıştı. İngilizlerin haberleşme istihbaratı ve kriptoanaliz alanındaki başarıları Birinci Dünya Savaşı'nın gidişatını nasıl şekillendirdiyse Bletchley Park'taki İngiliz operasyonunun

Almanya'nın Enigma ve Lorenz şifrelerini kırması da İkinci Dünya Savaşı'nın gidişatını şekillendirdi.

Enigma ve Lorenz şifreleme sistemleri, Almanya'nın "ele geçirilemez olarak kalacağına" inandığı mesajları şifrelemek için olağanüstü derecede karmaşık rotor makineleri kullanıyordu.[38] Her tuş vuruşu, bir karakteri makine için yapılan benzersiz ayarlara dayalı olarak başka bir karakter ile değiştiriyordu. Lorenz sisteminde sayısı evrendeki toplam atom sayısından fazla olan bu ayarların, mesajın okunabilmesi için gönderen ve alıcı arasında paylaşılması gerekiyordu.[39] Enigma; ordu, Gestapo ve diplomatlar tarafından kullanırken daha da karmaşık olan Lorenz, Adolf Hitler ve kıdemli Nazi askeri subayları arasında iletişim için kullanılıyordu.

İngilizlerin Enigma ve Lorenz'i kırma başarısı birçok gelişmenin bir sonucuydu. İlk olarak, bazı daha basit Enigma makinelerini kırmak için Almanların bazı hatalarından faydalanan Polonya ile müttefik istihbarat işbirliğinin bir sonucuydu.[40] Zamanın İngiliz kripto analiz uzmanlarından birinin dediği gibi, Polonya'nın katkıları olmadan çabaları "asla bir sonuca ulaşamazdı".[41]

İkinci olarak, Almanların kendilerine aşırı güvenmelerinin bir sonucuydu. Almanya şifrelerin kırıldığından hiçbir zaman şüphelenmedi ve bu nedenle, Britanya'yı en baştan başlamaya zorlayacak oldukça kolay değişiklikler bile yapılmadı.[42] Hal böyleyken bile, Bletchley Park'ın eski görevlilerinden biri, Almanların makinelerinin ele geçirilemez olduğuna güvenmesinin "neredeyse haklı" olduğunu söylüyor.[43]

Son olarak, Almanya'nın "telsiz disiplinindeki" tek bir büyük ihmal, makinenin kendisini asla görmeden Alman şifreleme sistemlerine ters mühendislik uygulamasına olanak sağlayan bir boşluk yarattı.[44] En karmaşık sistemler bile kullanıcı hatalarına karşı savunmasızdı ve dikkatli bir düşman bundan faydalanabilirdi.

Birleşik Krallık, Enigma ve Lorenz'i kırarak Almanya'nın en hassas iletişimlerinden bazılarına erişim elde etti. Winston Churchill'in bu istihbaratın Büyük Britanya'nın savaşı kazanmasının temel sebebi olduğunu söylediği, Dwight D. Eisenhower'ın ise bunu "belirleyici" olarak nitelendirdiği kabul ediliyor.[45] Britanya resmi istihbarat tarihçisi Sör Francis Harry Hinsely, bu başarıların " savaşı en az iki yıl, muhtemelen dört yıl kısalttığını", Afrika'da Mareşal Erwin Rommel'a zarar verdiğini, müttefiklerin gemi kayıpları karşısında Alman denizaltı kayıplarına yol açtığını ve Normandiya çıkartmalarına olanak sağladığını savunuyor.[46] Ayrıca Britanya'nın ülkeye giriş yapan tüm Alman casuslarını tespit etmesine ve bunları genellikle iade etmesine veya yanıltıcı istihbarat iletmek için kullanmasına olanak sağladı. Programın başındaki yetkili, İngiliz istihbaratının "bu ülkedeki Alman casusluk sistemini aktif bir şekilde yönettiğini ve kontrol ettiğini" ifade ediyor.[47] Savaş zamanında çok az sayıda ülke, bir diğer ülke hakkında bu kadar yakından bilgi edinebilmiştir.

Britanya'nın Almanya'ya yönelik çabalarının başarılı sonuçlanması, Polonya'nın barış zamanlarında Alman iletişimlerini izlemesi ve çığır açan buluşunu Büyük Britanya ile paylaşma kararı birlikte ele alındığında, günümüzde büyük güçlerin birbirlerine karşı yürüttükleri siber keşiflere uygulanabilecek dersler çıkarmak mümkün. Daha geniş kapsamlı olarak, şifrelemenin telekomünikasyon ağlarının düşman tarafından ele geçirilmesi sorununu hafiflettiğini iddia edenler, Almanya'nın bir zamanlar yaptığı hatadan çok da farklı olmayan bir hata yapıyor olabilir: teknolojiye haddinden fazla güvenme ve her zaman mevcut olan insan hatası ihtimaline yeterince dikkat etmeme.

## 6. Ivy Bells Operasyonu: Bilgi arayışının derinlikleri

*Bir Sovyet telefon hattına başlık takma çabalarına dahil olduğu aktarılan USS Halibut.*

*Kaynak: ABD Donanması / Wikimedia Commons*[48]

Sovyetler Birliği, şifreleme sistemleri konusunda Nazilerden çok daha dikkatliydi ve büyük ölçüde daha karmaşık olan kendi Enigma versiyonu Fialka'ya güveniyordu.[49] Bu nedenle, İkinci Dünya Savaşı'nda alman şifrelerinin kırılmasıyla elde edilen stratejik seviyedeki istihbarat hazinesine karşılık, Soğuk Savaş döneminde kamuoyunca bilinen benzer bir durum yaşanmadı. Bu zorluklar karşısında, düşmanın telekomünikasyon sistemlerine sızmak için başka yöntemler geliştirildi. Bu çabalardan en cesur olanlardan biri, sualtı kabloları alanında görüldü.

19. yüzyılda sualtı kablolarının ortaya çıkması sonucunda bu kabloları kesme ve bunlara dinleme başlığı takma çabaları da görülmeye başlandı. Bu, genellikle bu tür görevleri gerçekleştirmenin kolay olduğu sığ sularda yapılıyordu. Bu tür operasyonları düşman kontrolündeki derin sularda gerçekleştirmek ise hele ki gizli yapılması gerektiği düşünüldüğünde hemen hemen imkansız görülüyordu. 20. yüzyıldan itibaren, İngilizler ve ardından gelen büyük güçler sualtı kablolarının güvenliği hakkında bir sonuca varmıştı: Karaya çıkarma alanları güvenliyse ve kablolar tarafsız ya da hasmane ülkelerin topraklarından geçmiyorsa genellikle ele geçirmeye karşı güvenli ve özellikle de barış zamanlarında kesilmeye karşı güvende demekti.[50]

Soğuk Savaş sırasında bu hesap değişti. Nükleer denizaltıların icat edilmesi, daha derin sulardaki sualtı kablolarına başlık takma imkanını doğurdu. Ancak dalgıçları derin deniz tabanındaki kablolara erişme görevine göndermek, daha önceki çağlarda denenen bilindik kablo manipülasyonu çabalarından ziyade uzay keşiflerine benziyordu. Bu koşullarda takılabilecek bir dinleme başlığı geliştirmek teknik olarak da zordu.

Amerika Birleşik Devletleri'nin, Vladivostok'taki donanma karargahından Kamchatka yarımadasındaki bir denizaltı üssüne giden bir Sovyet sualtı kablosu olabileceğinden şüphelendiğinde bu engelleri aşmaya çalışması, haberleşme istihbaratının değerini ortaya koyuyor.[51] 13 cm'lik kablo demetine dinleme başlığı takılmasının Sovyet nükleer güçleri hakkında kritik bilgiler sağlayacağına inanılıyordu.[52] Sovyetler, havadan gönderilen tüm trafiği şifreliyordu ancak Amerika Birleşik Devletleri, Sovyetlerin korumalı sualtı kabloları üzerinden gönderilen trafiğe erişmenin hemen hemen imkansız olduğunu varsayacağını ve bu nedenle şifrelemeyeceğini umuyordu. Ayrıca, "Sovyet amiraller ve generaller, ellerindeki iş yükü altında zaten ezilen kriptografları bekleyemeyecek kadar sabırsız ve buyurgandı" ve güvenliksiz sesli iletişim konusunda ısrarcıydı.[53] Bir dinleme başlığı ender bir istihbarat hazinesi sağlayabilirdi, bu nedenle ABD Donanması Ivy Bells operasyonunu başlattı.

Dinleme başlığı ve bundan elde edilen istihbarat hâlâ çok gizli bilgi kategorisinde ancak açık kaynaklar, bu benzersiz ve yenilikçi operasyon konusunda ayrıntılar veriyor. Amerika Birleşik Devletleri, Sovyet donanmasını sinsice atlatarak 600.000 mil karelik bir alana yayılmış sualtı kablolarını bulmak için USS Halibut adlı bir nükleer denizaltını görevlendirdi.[54] Dalgıçların yüksek basınçlar altında ve aşırı soğuk sularda saatler boyunca çalışabilmesi için yenilikçi teknolojiler geliştirildi. Benzer şekilde, bu zorlu ortamda dinleme başlığı takmak için yeni yöntemler geliştirildi.[55] Tüm bunların Sovyetler farkına varmadan veya şüphelenmeden yapılması gerekiyordu. Gemi fark edilseydi Sovyetler gemiye çıkabilir veya gemiyi imha edebilirdi.

Operasyon başarılı oldu ve 1970'ler boyunca ABD Donanması bu kablo üzerindeki şifrelenmemiş mesajları dinleyerek kayda aldı. Birkaç ayda bir Amerikan denizaltıları, taarruz denizaltılarından kaçarak sessizce Sovyet sularına sızıyor, dalgıçları başlık takılan kablo hatlarına gönderiyor ve Sovyet iletişimlerinin kasetlerini alıyordu. Bu, son derece değerli ve nadir bir istihbarat kaynağıydı. Amerika Birleşik Devletleri haberleşme istihbaratı almak için bir "casus uydular, uçaklar, dinleme istasyonları ve denizaltılar ağına" sahip olsa da bir düşmanın topraklarındaki "fiziki telefon hattına sızamıyordu". Bu çaba, telekomünikasyonda evrimsel bir dönüşüme işaret ediyordu: Hangi ortamda ve hangi yöntemle gönderilirse gönderilsin, iletilen veriler ve haberleşmelere doğru araçlar ve yeterli azimle erişmek mümkündü. Bu dinleme nihayetinde bir sızdırma sonucu açığa çıkmış olsa da elde edilen telekomünikasyon bilgileri Amerika Birleşik Devletleri'ne ve müttefiklerine paha biçilemez askeri ve siyasi istihbarat sağladı.[56]

## Tarih perspektifinden modern telekomünikasyon yarışı

Soğuk Savaş sona erdiğinde, Amerika Birleşik Devletleri bilgi hegemonyasında Büyük Britanya'nın yerini net bir şekilde almıştı. Amerika Birleşik Devletleri küresel internette kilit bir konum, güçlü uzay yetkinlikleri, birçok internet teknolojisine hakimiyetin yanı sıra kamuoyu bilgilendirmelerinde açıklandığı üzere, düşman iletişimlerini ele geçirme veya engellemeye yönelik sofistike imkanlara sahipti.

Amerika'nın sahip olduğu bu avantajlar, tıpkı yüz yıl önce Büyük Britanya'ya olduğu gibi, sarsılmak üzere. Rusya ve özellikle Çin, artık ABD hakimiyetine meydan okuyor. Amerika Birleşik Devletleri birçok bilgi akışında hâlâ kilit konumunu korusa da diğer güçler ABD ağlarına bağımlılıklarını azaltmanın yollarını her geçen gün daha fazla arıyor. Aynı zamanda, Amerika'nın kilit konumu, ele geçirme amaçları bakımından yüz yıl önce Büyük Britanya için olduğu kadar gerekli değil. İnternet, fiziksel altyapının kontrolünü ele geçirmeden sızmayı mümkün kılıyor. Akıllı telefonlar ve bilgisayar ağları heklenebiliyor ve hassas iletişimler ister geçmiş çağın fiziksel dinleme başlıklarıyla ister modern çağın sanal sızmalarıyla ele geçirilmiş olsun sonuç aynı oluyor. Bu şekilde bağlantılı olmak, telgraf ve kablosuz telsiz çağına kıyasla şu anda çok daha fazla riske açık.

Rusya, bu riske açık olma durumunu en fazla suistimal eden devlet. 2007 yılında Rusya, Estonya kurumlarına karşı çoğu dağıtılmış hizmet dışı bırakma saldırıları olan bir siber saldırı dalgası başlattı.[57] 2008'de, Rusya-Gürcistan Savaşı'nda siber saldırılar gerçekleştirdi. Bunlar yalnızca yönlendirmeli hizmet dışı bırakma saldırılarını değil, aynı zamanda hükümet web sitelerini yönlendirme, Gürcistan devlet sunucularını ele geçirme ve Gürcistan'ın internet trafiğini Rusya kontrolündeki sunucular üzerinden yönlendirme çabalarını içeriyordu ve saldırılardan bazıları, Rusya'nın askeri hamlesiyle eş zamanlı olacak şekilde çatışma öncesi gerçekleştiriliyordu.[58] 2014 yılında Rusya Kırım'ı işgal ettiğinde, siber saldırıları telekomünikasyon ağlarının fiziksel kontrolüyle birleştirdi. Rus askerleri, Ukrayna'nın telekomünikasyon tesislerine el koyarak bunları Kırım'da iletişimi kesmek ve hatta Ukrayna'nın diğer bölgelerinde siber saldırılar ve kargaşa yaratmak için kullandı.[59] Rusya, 2015'te Ukrayna altyapılarını hedef alan bir siber saldırı dalgası başlatarak iki kez yüzbinlerce Ukraynalının elektriğini kesti. Takip eden birkaç yıl boyunca, "medya, finans, ulaşım, ordu, politika ve enerji" dahil olmak üzere Ukrayna toplumunun hemen hemen her kesimini hedef alan benzeri görülmemiş bir saldırı dalgası başlattı. Bazıları bunu, Amerika Birleşik Devletleri'ne karşı benzer bir mücadeleye hazırlık olarak yorumladı.[60] Aynı zamanda, Baltık Devletleri'ne karşı saldırıları da sürdürerek dezenformasyon kampanyalarıyla başka ülkelerin yanı sıra 2016 ve 2020 yıllarında ABD seçimlerine yön vermeye çalıştı.[61] 2021'de ABD hükümeti, Rusya'yı BT şirketi SolarWind'i heklemekle resmi olarak suçladı. Bu, federal hükümetin çoğunu ve birçok büyük ABD şirketini tehlikeye atan sofistike bir saldırıydı.[62]

Telekom yarışına ciddi yatırımlar yapan bir diğer büyük güç ise Çin. Ancak Rusya'nın aksine Çin'in çabaları yalnızca mevcut internet altyapısını suistimal etmeyi değil aynı zamanda etkileyebileceği ve hatta kontrol edebileceği ağlar ve altyapılar kurmayı da amaçlıyor. Rusya gibi Çin de internetin riske açıklığından ustalıkla faydalanıyor. Çin, 2000'lerin başlarında ABD Savunma Bakanlığı ağlarına bir saldırı dalgası başlattı. Bakanlık, bu saldırılara Titan Yağmuru Operasyonu adını vermişti.[63] Dünya genelinde Amerika Birleşik Devletleri, Birleşik Krallık,

Fransa, Almanya, Kanada, Avustralya, Japonya, Güney Kore, Tayvan, Hindistan ve bir düzine diğer ülkenin hükümetleri, Çin'in hükümet ağlarına sızmasından şikayetçi. Geçtiğimiz on yılın en büyük siber saldırılarından birinin Çinli taraflarca gerçekleştirildiği, ABD Adalet Bakanı General William Barr tarafından doğrulandı. Saldırı, ABD Personel Yönetimi Ofisi'nden (21 milyon kişinin kayıtları), Marriott otellerinden (400 milyon), Anthem sağlık sigortası şirketinden (80 milyon) ve Equifax'ten (147 milyon) ve başka kuruluşlardan kayıtların çalınmasını içeriyordu.[64]

Aynı zamanda, Çin geleceğin internet altyapısının da temellerini atıyor ve önceki çabaları düşünüldüğünde bu çabanın şu anda ticari olması veya önümüzdeki dönemde tamamen ticari nitelikli kalması pek olası değil. Çin'in yatırımları sayısız cihazı ve sensörü birbirine bağlayan daha akıllı, bağlantılı bir ekonominin temellerini oluşturması beklenen 5G üzerine yoğunlaşıyor. Dünya genelinde bu ağları oluşturmaya çok istekli olan Çin, "Dijital İpek Yolu" inisiyatifi kapsamında dünya genelinde 5G lider şirketleri ve projelerine sübvansiyonlar sağlıyor. Rekabetçi fiyatlandırma ile Huawei gibi şirketler diğer büyük 5G tedarikçilerini geride bırakmayı başararak önemli bir küresel pazar payı elde etti ve Çin'i bu ağların oluşturulmasında lider haline getirdi. 5G dışında da Çin hükümeti hemen hemen her kıtada internet veya iletişim altyapısı kurma çalışmalarına da finansal destek sağladı. Bu çabaların tümü, Çin için üst düzey planlama belgeleriyle güvence altına alınan temel bir politika önceliği olan küresel standartları şekillendirme kampanyası ile destekleniyor. Yüz yıl önceki İngiliz-Alman rekabetinde olduğu gibi bu, telekomünikasyonun geleceğini Çin lehine şekillendirebilir. Bu amaçla Çin, yeni bir veri güvenliği inisiyatifi açıkladı.[65]

Bazıları, Çin'in faaliyetleri sayesinde Pekin hükümetinin ister trafiği ele geçirme ister hizmet dışı bırakma amacıyla bu ağların kontrolünü fiili olarak ele geçirmesi ihtimalinden endişe duyuyor. Çin'in bu kontrolü ele geçirme çabalarıyla ilgili kamuya çok az bilgi açıklansa da ABD hükümeti Şubat 2020'de Huawei'in ağ ekipmanlarında arka kapılar bulunduğunu, bunu sözleşme yapmış olduğu ilgili şirketlere açıklamadığını ve bu arka kapıların ev sahibi hükümetler tarafından yasal dinlemeler kapsamında bazen talep edilen seviyenin ötesinde olduğunu ortaya çıkardı.[66] Ayrıca, kamu bilgilendirmelerinde Huawei'in Uganda ve Zambiya gibi hükümetlere muhaliflerin kimliklerini açığa çıkarmada yardımcı olduğu ortaya çıktı.[67] Huawei örneğinin de ötesinde, bir siber güvenlik firması Çin hükümetinin yabancı şirketlerin kurmasını istediği zorunlu bir vergi yazılımında da arka kapılar olduğunu keşfetti.[68] Bu örneklerin Huawei'in bu ağlardaki konumunu suistimal ettiği anlamına gelip gelmediğinden bağımsız olarak, şirketin davranışları ve Çin'in siber saldırı ve casusluk alanındaki sabıkası endişelere neden oluyor.

Diğer başlıca endişe nedenleri, tarihe ve kanunlarla daha kapsamlı bir şekilde sınırlandırılan daha liberal büyük güçlerin bile geçmişteki davranışlarına dayanıyor. Gerçekten de tarihte görülen örnekler, Huawei gibi bir şirketin kullanabileceği türde bir güç ve nüfuzun Çin hükümeti tarafından suistimal edilebileceğini düşündürüyor. Tıpkı diğer büyük güçlerin şirketlerinin konumlarını veya telekomünikasyondaki imkanlarını suistimal ettikleri gibi.

Daha geniş bir tarihsel açıdan bakıldığında, şirketin amacı tamamen ticari de olsa, "arka kapı ve casusluk olmaması" sözü inandırıcı bile olsa ve Pekin bu sözleri tutma taahhüdünde samimi bile olsa kanıtlar Huawei'in telekomünikasyon ağlarındaki rolü hakkında ihtiyatlı olunması gerektiğini gösteriyor.

Bu raporun gösterdiği gibi daha geniş bir açıdan bakıldığında, büyük güçlerin telekomünikasyon yarışının bugün yeni gibi görünen özelliklerinin aslında geçmişte de kökleri mevcut. Tarih boyunca, birçok tema kendini tekrar ediyor:

- *Güç:* Telekomünikasyon ağlarının kontrolü, 150 yıl önce ilk ortaya çıkışından bu yana bir siyasi güç biçimi olageldi. Büyük Britanya telekomünikasyon ve telsiz alanlarındaki rolünü suistimal etti, benzer şekilde Amerika Birleşik Devletleri de modern internet çağında aynısını yaptı ve Çin'in de bugün bunu yapabileceğinden endişe duymak için sebep var.

- *Rehavet*: Uzun süren barış ve refah dönemleri, telekomünikasyon riskleri konusunda rehavete yol açtı. 19. Yüzyıl'da büyük güçler yabancı şirketlere ve dış ülkelerin işlettiği ağlara güvenmekten memnundu. Tıpkı günümüzde devletlerin Çin'in telekomünikasyon ekipmanlarını ve operasyonlarını kabul etmeye istekli olduğu gibi. Fakat nihayetinde, olası rakiplere ve düşmanlara güvenmek Almanya gibi ülkeler için felaketle sonuçlandı ve dünya siyasetinin akışını değiştirdi.

- *Suistimal:* Yeni telekomünikasyon teknolojileri her zaman bu teknolojileri ele geçirmeye, hizmet dışı bırakmaya veya suistimal etmeye yönelik çabaları da beraberinde getirdi. Şifrelemenin Çin'in modern iletişimleri dinleme çabalarını zorlaştırabileceği umulsa da geçmiş dönemlerde şifrelemeye büyük umutlar beslendiğinde kullanıcı hatası ve rakip devletlerin kararlı çabalarının bunları kırabildiği görüldü. Büyük Britanya "kırılamaz" olduğu düşünülen şifrelerini kırmayı başardığında Almanya'nın başına geldiği gibi. Güvenli olduğu varsayılan her teknoloji dalgası konusunda biraz mütevazı olmakta yarar var.

- *Lider şirketler:* Devletler, özellikle de büyük güçler arasında gerilim arttığında kendi telekomünikasyon liderlerini yaratmaya çalışır. Çin hükümeti, Huawei'in başarılarından gurur duyuyor ve bu şirketi tüm dünyada destekliyor, hatta teknolojisini reddeden devletleri tehdit ediyor. Tarih boyunca birçok diğer telekomünikasyon lideri devlet baskısından uzak kalamamışken, hükümetine bu kadar yakın olan bir şirketin devlet baskısından uzak olması pek de olası değil.

- *Standartlar*: Telekomünikasyon standartları ağ gücünü kimin kullanacağını belirleyebilir. Almanya'nın Büyük Britanya'nın kablosuz telsiz hakimiyetini kırmak için standart belirleyici bir kuruluş kullanması gibi. Günümüzde bu yarış, Uluslararası Telekomünikasyon Birliği gibi organlarda yer buluyor ve Huawei'in buradaki rolü, standartlarının Çin'in telekomünikasyonu yeniden şekillendirmesine olanak sağlama ihtimalini dikkate almak gerekiyor.

- *Hizmet dışı bırakma:* Ağ güvenliği, yalnızca ele geçirme ve veri güvenliğinden ibaret değildir, aynı zamanda tüm bir ağın hizmet dışı bırakılmasını veya dış ağlara erişimi de kapsar. Büyük Britanya Almanya'nın dünya telgraf ağlarıyla bağlantısını kesmiştir ve Huawei'in ağlardaki rolü, verilere kolayca erişemese bile ekipman operasyonlarını yürüttüğü ülkelerde ağları kapatma gücü verebilir.

- *Kararlılık:* Birçok devlet, iletişim ağlarını ele geçirmek için düşmanlarının ne derecede çaba gösterebileceğini genellikle hafife alır ve sonrasında nahoş sürprizlerle karşılaşır. Britanya'nın endüstriyel düzeyde çabalarla İkinci Dünya Savaşı'nda Alman şifrelerini kırmayı başarması ve Amerika'nın dinlemez olduğu düşünülen Sovyet sualtı kablolarına dinleme başlığı takma başarısı, büyük güçlerin kritik haberleşme istihbaratına erişmek için neleri göze alabileceğini gösteriyor. Çin'in de bu tür büyük çabalar sarf etmesi muhtemeldir. Huawei, modern ağlardaki konumunu silaha dönüştürmekte zorlansa bile Çin gibi kararlı bir rakibin motivasyonunu ve sahip olduğu kaynakları küçümsemek telekomünikasyon yarışında tarihi örneklerin tekrarına yol açacaktır.

Bu raporun gösterdiği gibi, taraflar değişmiş olsa da büyük güçlerin telekomünikasyon yarışının birçok özelliği aynı kalmış durumda.

## Yazarlar Hakkında

**Rush Doshi**, Brookings Çin Stratejisi Girişimi'nin yöneticisiydi ve Brookings Dış Politika'da araştırmacı olarak görev aldı. Ayrıca Yale Hukuk Fakültesi'nin Paul Tsai Çin Merkezi'nde araştırmacı olarak çalıştı ve Wilson China üyeleri açılış dersinde yer aldı. Araştırmalarında Çin'in büyük stratejisine ve Hint-Pasifik güvenlik sorunlarına odaklanmıştır. Doshi, Oxford University Press tarafından yayımlanacak olan *The Long Game: China's Grand Strategy to Displace American Order* [Uzun Oyun: Çin'in Amerikan Düzeninin Yerini Almak İçin Büyük Stratejisi] adlı kitabın yazarıdır. Şu anda Biden hükümetinde görev almaktadır.

**Kevin McGuiness** Savunma Bakanlığı Skillbridge Programı'ndan bir dış taraf olarak yakın zamanda Brookings ile birlikte çalışmış, bu kapsamda Doğru Asya Politikası Araştırmaları Merkezi'nde çeşitli projelere katkı sağlamıştır. Hava Kuvvetleri'nde görev yapmış ve Amerika Birleşik Devletleri Hava Kuvvetleri Akademisi'nde Asya siyasetinde uluslararası ilişkiler derslerini yönettiği öğretim üyeliği görevini kısa süre önce tamamlamıştır. Ayrıca yakın zamanda Ulusal Strateji Araştırmaları Enstitüsü'nün Çin Askeri Araştırmaları Merkezi'nde araştırma görevlisi olarak çalışmış, PLA modernizasyonu ve Hint Pasifiği'nde güvenlik konularına odaklanmıştır.

## Teşekkür

Yazarlar, bu projedeki araştırma destekleri için eski stajyerler Isabella Lu, Gaoqi Zhang ve Zijin Zhou'ya; bu makaleyi yayıma hazırladıkları için pek çok isimsiz redaktöre, Claire Harrison ve Ted Reinert'a ve mizanpaj ve web tasarım desteği için Chris Krupinski ve Rachel Slattery'ye teşekkür eder. Brookings, bu araştırmanın finansmanı için ABD Dışişleri Bakanlığı'na ve Institute for War and Peace Reporting'e teşekkür borçludur.

*Bu rapor, Rush Doshi'nin hükümette görev almasından önce tamamlanmıştır, yalnızca açık kaynaklardan yararlanılmıştır ve ABD hükümetinin hiçbir kurumunun resmi politikasını veya konumunu yansıtmamaktadır.*



[1] Steven Chase, Robert Fife ve Barrie McKenna, "Trudeau Refuses to Let 'politics Slip into' Decision on Huawei" [Trudeau, Siyasetin Huawei ile İlgili Kararlara Karıştırılmasını İstemiyor], The Globe and Mail, 15 Ekim 2018, https://www.theglobeandmail.com/politics/article-trudeau-refuses-to-let-politics-slip-into-decision-on-huawei/; Greg Quinn ve Josh Wingrove, "Trudeau Says Politics Won't Factor Into Huawei 5G Decision" [Trudeau, Huawei 5G Kararına Siyasetin Dahil Olmayacağını Söylüyor], Time, 19 Aralık 2018, https://time.com/5485141/justin-trudeau-huawei-5g-decision-politics/.

[2] Daniel R. Headrick, The Invisible Weapon: Telecommunications and International Politics: [Görünmez Silah: Telekomünikasyon ve Uluslararası Siyaset], 1851-1945 (Oxford, Birleşik Krallık: Oxford University Press, 1991), bölüm 1.
[3] A.g.e., bu gözlem Headrick'e aittir.
[4] A.g.e
[5] A.g.e
[6] A.g.e., bu gözlem Headrick'e aittir.
[7] Heidi Tworek, News from Germany: The Competition to Control World Communications: [Almanya'dan Haberler: Dünya İletişimlerini Kontrol Etme Yarışı], 1900-1945 (New York: Harvard Historical Studies, 2019).
[8] Daniel R. Headrick, The Invisible Weapon [Görünmez Silah].
[9] "NH 79949 Cienfuegos Cable-Cutting Operation, 11 May 1898" [NH 79949 Cienfuegos Kablo Kesme Operasyonu, 11 Mayıs 1898], Naval Historical Center Çevrimiçi Kütüphanesi, https://www.history.navy.mil/content/history/nhhc/our-collections/photography/us-people/b/baker-benjamin-f/nh-79949.html.
[10] A.g.e., bölüm 5.
[11] Jonathan Winkler, "Information Warfare in World War I" [Birinci Dünya Savaşı'nda Bilgi Savaşı], The Journal of Military History 73, no. 3 (2009): 845–67, https://doi.org/10.1353/jmh.0.0324.
[12] Cameron McR. Winslow, "Cable-Cutting at Cienfuegos" [Cienfuegos'da Kablo Kesimleri], The Century Illustrated Monthly Magazine 57 (1899): 708-717, https://books.google.com/books?id=Y7fPAAAAMAAJ&pg=PA708#v=onepage&q&f=false.
[13] Jonathan Winkler, "Silencing the Enemy: Cable-Cutting in the Spanish–American War" [İspanyol-Amerikan Savaşı'nda Kablo Kesimleri], War on the Rocks, 6 Kasım 2015, https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/; Rebecca Raines, "Manifesting Its Destiny: The U.S. Army Signal Corps in the Spanish-American War" [Kaderini Şekillendirme: İspanyol-Amerikan Savaşı'nda ABD Ordusu Haberleşme Kuvvetleri], *Army History* 46 (1998): 14–21, https://www.jstor.org/stable/26304991.
[14] Jonathan Winkler, "Silencing the Enemy" [Düşmanı Susturma].
[15] "Spanish American War: Telegraphy and Cable Cutting, Introductory Essay" [İspanyol-Amerikan Savaşı: Telgraf ve Kablo Kesimleri, Giriş Makalesi], Naval History and Heritage Command, https://www.history.navy.mil/research/publications/documentary-histories/united-states-navy-s/telegraphy-and-cable.html.
[16] Jonathan Winkler, "Silencing the Enemy" [Düşmanı Susturma].
[17] Library of Congress, George Grantham Bain Collection [Kongre Kütüphanesi, George Grantham Bain Koleksiyonu], https://www.loc.gov/pictures/item/2014683102/.
[18] Ancak Heidi Tworek'in de belirttiği gibi, bu teknolojinin geliştirilmesinde mucidin kendi rolü biraz abartılmıştır. Heidi Tworek, *News from Germany [Almanya'dan Haberler]*.
[19] Marc Raboy, "The First Company That Wanted to 'Connect the World' Wasn't Google or Facebook" ['Dünyayı Bağlantılı Hale Getirmek' İsteyen İlk Şirket Google veya Facebook Değildi], Media@LSE, 24 Ağustos 2016, https://blogs.lse.ac.uk/medialse/2016/08/24/the-first-company-that-wanted-to-connect-the-world-wasnt-google-or-facebook/.
[20] Heidi Tworek, News from Germany [Almanya'dan Haberler], 12–13.
[21] Michael Friedewald, "Telefunken vs. Marconi, or the Race for Wireless Telegraphy at Sea" [Telefunken ve Marconi ya da Denizde Telsiz Telgraf Yarışı, 1896-1914], SSRN (9 Ocak 2014): https://doi.org/10.2139/ssrn.2375755.
[22] A.g.e
[23] Marc Raboy, Marconi: The Man Who Networked the World [Marconi: Dünyayı Ağlarla Birbirine Bağlayan Adam] (Oxford, Birleşik Krallık: Oxford University Press, 2016), 226–28.
[24] Örneğin, Telefunken Almanya'nın büyük bir koloni varlığına sahip olmadığı Latin Amerika gibi bölgelerde bile aktifti.
[25] George Johnson, ed., *All Red Line: The Annals and Aims of the Pacific Cable Project [All Red Line: Pasifik Kablo Projesinin Tarihi ve Amaçları]* (Ottawa: James Hope and Sons, 1903), 10, İnternet Arşivi, https://archive.org/details/allredlineannals00johnuoft/page/n11/mode/2up.
[26] Gordon Corera, "How Britain Pioneered Cable-Cutting in World War One" [Britanya Birinci Dünya Savaşı'nda Kablo Kesmede Nasıl Öncü Oldu?], BBC News, 15 Aralık 2017, https://www.bbc.com/news/world-europe-42367551.
[27] Jonathan Winkler, "Information Warfare in World War I" [Birinci Dünya Savaşı'nda Bilgi Savaşı], 847.

[28] P. M. Kennedy, "Imperial Cable Communications and Strategy, 1870-1914" [Emperyal Kablo İletişimi ve Stratejisi, 1870-1914], The English Historical Review 86, no. 341 (1971): 728–52, https://www.jstor.org/stable/563928.
[29] Jonathan Winkler, "Information Warfare in World War I" [Birinci Dünya Savaşı'nda Bilgi Savaşı], 849.
[30] A.g.e., 851.
[31] Gordon Corera, "Why Was the Zimmermann Telegram so Important?" [Zimmermann Telgrafı Neden Bu Kadar Önemliydi?], BBC News, 17 Ocak 2017, https://www.bbc.com/news/uk-38581861; Patrick Beesly, Room 40: İngiliz Deniz İstihbaratı 1914-18 (San Diego: Harcourt Brace Jovanovich, 1982).
[32] C. O. Nordensvan ve Valdemar Langlet, *Det stora världskriget* [Büyük Dünya Savaşı] (1915), Wikimedia Commons, https://commons.wikimedia.org/wiki/File:German_WW_I_field_telegraph_002.jpg.
[33] Jonathan Winkler, "Information Warfare in World War I" [Birinci Dünya Savaşı'nda Bilgi Savaşı].
[34] Wilhelm Flicke, "The Beginnings of Radio Intercept in World War I: A Brief History by a German Intelligence Officer" [Birinci Dünya Savaşı'nda İlk Telsiz Ele Geçirme Adımları: Bir Alman İstihbarat Subayından Kısa Bir Tarih], NSA Cryptologic Spectrum Articles 8, no. 2 (1978): 21, https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/.
[35] Bruce Norman, Secret Warfare: The Battle of Codes and Ciphers [Gizli Savaş: Kod ve Şifre Muharebesi] (Newton Abbot, Birleşik Krallık: David & Charles Ltd, 1973); Prit Buttar, Collision of Empires: The War on the Eastern Front in 1914 [İmparatorlukların Çarpışması: 1914'te Doğu Cephesindeki Savaş] (Oxford, İngiltere: Osprey Publishing, 2014).
[36] Matt Crypto, "The rotors of a Lorenz SZ42 cipher machine on display at Bletchley Park museum" [Bletchley Park müzesinde sergilenen bir Lorenz SZ42 şifre makinesinin rotorları], Wikimedia Commons, https://commons.wikimedia.org/wiki/File:SZ42-6-wheels.jpg.
[37] George I. Beck, "Military Communication - The Advent of Electrical Signaling" [Askeri İletişim: Elektrikli Haberleşmenin Ortaya Çıkışı], Britannica, https://www.britannica.com/technology/military-communication.
[38] Harry Hinsley, "The Influence of ULTRA in the Second World War" [İkinci Dünya Savaşı'nda ULTRA Etkisi] (ders, Cambridge, Birleşik Krallık, 19 Ekim 1993), http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF.
[39] $1x10^{170}$ ayar olasılığı.
[40] "Bletchley Park Remembers Polish Code Breakers" [Bletchley Park, Polonyalı Kod Kırıcıları Hatırlıyor], BBC News, 14 Temmuz 2011, https://www.bbc.com/news/uk-england-beds-bucks-herts-14141406.
[41] Gordon Welchman, The Hut Six Story: Breaking the Enigma Codes [Hut Six Hikayesi: Enigma Kodlarını Kırma] (Cleobury Mortimer, Birleşik Krallık: Classic Crypto Books, 1997).
[42] Harry Hinsley, "The Influence of ULTRA" [ULTRA Etkisi].
[43] A.g.e
[44] Örneğin, bkz. Jerry Roberts, Lorenz: Breaking Hitler's Top Secret Code at Bletchley Park [Lorenz: Bletchley Park'ta Hitler'in Çok Gizli Kodunun Kırılması] (Cheltenham, Birleşik Krallık: History Press, 2017).
[45] F. W. Winterbotham, The Ultra Secret [Ultra Sır] (New York: Harper & Row, 1974), 154, 191.
[46] Harry Hinsley, "The Influence of ULTRA" [ULTRA Etkisi].
[47] Calder Walton, "The Spies Who Came In From the Continent" [Anakaradan Gelen Casuslar], Foreign Policy, 27 Nisan 2019, https://foreignpolicy.com/2019/04/27/the-spies-who-came-in-from-the-continent-espionage-britain-brexit/.
[48] ABD Donanması, Wikimedia Commons, https://commons.wikimedia.org/wiki/File:USS_Halibut_with_bow_thruster.jpg.
[49] Anna Borshchevskaya, "The Soviets' Unbreakable Code" [Sovyetlerin Kırılamayan Kodu], Foreign Policy, 27 Nisan 2019, https://foreignpolicy.com/2019/04/27/the-soviets-unbreakable-code-fialka-encryption-espionage-russia-kgb-spy/.
[50] Daniel R. Headrick, The Invisible Weapon [Görünmez Silah], bölüm 4.
[51] Sherry Sontag, Christopher Drew ve Annette Lawrence Drew, Blind Man's Bluff: The Untold Story of American Submarine Espionage [Kör Adamın Blöfü: Amerikan Denizaltı Casusluğunun Anlatılmamış Hikayesi] (New York: Public Affairs, 1998), 222.
[52] A.g.e
[53] A.g.e., 223.
[54] A.g.e
[55] Matt Blitz, "Navy Divers and Their Daredevil Mission to Spy on the Soviet Union at the Bottom of the Sea" [Donanma Dalgıçları ve Deniz Tabanında Cüretkar Sovyetler Birliği Casusluğu Görevleri], Popular Mechanics, 30

Mart 2017, https://www.popularmechanics.com/technology/security/a25857/operation-ivy-bells-underwater-wiretapping/.

[56] Michael J. Sulick, American Spies: Espionage Against the United States from the Cold War to the Present [Amerikan Casusları: Soğuk Savaştan Bugüne Amerika Birleşik Devletlerine Karşı Casusluk] (Washington, DC: Georgetown University Press, 2013), 109–14; Matt Blitz, "Navy Divers" [Donanma Dalgıçları].

[57] Damien McGuinness, "How a Cyber Attack Transformed Estonia" [Bir Siber Saldırı Estonya'yı Nasıl Dönüştürdü?], BBC News, 27 Nisan 2017, https://www.bbc.com/news/39655415; Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia From the Information Warfare Perspective" [Estonya'ya Yönelik 2007 Siber Saldırılarının Bilgi Savaşı Perspektifinden Analizi], (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2008), https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/.

[58] David Hollis, "Cyberwar Case Study: Georgia 2008" Siber Savaş Vaka İncelemesi: Gürcistan 2008], Small Wars Journal, 6 Ocak 2011, https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008; Ronald J. Deibert, Rafal Rohozinski ve Masashi Crete-Nishihata, "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war" [Siber alanda tufanlar: 2008 Rusya-Gürcistan savaşında bilgi şekillendirme ve hizmet dışı bırakma], Security Dialogue 43, no. 1 (2012): 3–24, https://journals.sagepub.com/doi/10.1177/0967010611431079.

[59] Pavel Polityuk ve Jim Finkle, "Ukraine Says Communications Hit, MPs Phones Blocked" [Ukrayna İletişimlerin Hedef Alındığını, Milletvekillerinin Telefonlarının Bloke Olduğunu Söylüyor], Reuters, 4 Mart 2014, https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R220140304; Sergey Sukhankin, "Russian Electronic Warfare in Ukraine: Between Real and Imaginable" [Rusya'nın Ukrayna'daki Elektronik Savaşı: Gerçek ve Hayal Edilebilir Arasında], Jamestown Foundation, 24 Mayıs 2017, https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/.

[60] Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar" [Bir Ulus Nasıl Rusya'nın Siber Savaş Test Laboratuvarına Dönüştü?], Wired, 20 Haziran 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace" [Altı Rus GRU Subayı İmha Edici Kötü Amaçlı Yazılımlar ve Siber Alanda Diğer Bozucu Eylemlerle Bağlantılı Olarak Suçlanıyor], ABD Adalet Bakanlığı, 19 Ekim 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[61] Constanze Stelzenmüller, "The impact of Russian interference on Germany's 2017 elections" [Rusya'nın 2017 Almanya seçimlerine müdahalesinin etkisi], (kongre ifadesi, 28 Haziran 2017), https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

[62] Maggie Miller, "US intel agencies blame Russia for massive SolarWinds hack" [ABD istihbarat birimleri SolarWinds'in heklenmesinden Rusya'yı sorumlu tutuyor], *The Hill,* 5 Ocak 2021, https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwinds-hack.

[63] "Connect the Dots on State-Sponsored Cyber Incidents - Titan Rain" [Devlet Destekli Siber Olaylarda Noktaları Birleştirme: Titan Yağmuru], Dış İlişkiler Konseyi, https://www.cfr.org/cyber-operations/titan-rain.

[64] Garrett Graff, "China's Hacking Spree Will Have a Decades-Long Fallout" [Çin'in Hekleme Dalgasının Etkisi Onlarca Yıl Sürecek], Wired, 11 Şubat 2020, https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/.

[65] Chun Han Wong, "China Launches Initiative to Set Global Data-Security Roles" [Çin, Küresel Veri Güvenliği Rolleri Belirleme İnisiyatifi Başlattı], *The Wall Street Journal,* 8 Eylül 2020, https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974.

[66] Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks" [ABD Yetkilileri Huawei'in Telekom Ağlarına Gizlice Erişebildiğini Söylüyor], 12 Şubat 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

[67] Joe Parkinson, Nicholas Bariyo ve Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents" [Huawei Teknisyenleri Afrika Hükümetlerinin Siyasi Muhalifler Üzerinde Casusluk Yapmasına Yardım Etti], The Wall Street Journal, 15 Ağustos 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[68] William Turton, "Hidden Back Door Embedded in Chinese Tax Software, Firm Says" [Firma Çin'in Vergi Yazılımında Gömülü Gizli Arka Kapılar Olduğunu Söylüyor], Bloomberg, 25 Haziran 2020, https://www.bloomberg.com/news/articles/2020-06-25/hidden-back-door-embedded-in-chinese-tax-software-firm-says.