Huawei upoznaje povijest: Velike moći i rizik telekomunikacija, 1840. – 2021.

Rush Doshi i Kevin McGuiness

Brookings Institution, ožujak 2021.

Sažetak

Krajem 2018. godine, usred američke zabrinutosti hoće li Kanada izraziti tvrtki Huawei dobrodošlicu među svoje telekomunikacijske mreže, kanadski premijer Justin Trudeau dao je niz izjava koje su utjelovile opće mišljenje većeg dijela svijeta. „To ne bi trebala biti politička odluka“, izjavio je tad, a Kanada neće „dopustiti politici uplitanje u odluke“ o ulozi tvrtke Huawei u svojoj mrežnoj infrastrukturi.[1]

Ideja da se politika moći može ukloniti iz pitanja o telekomunikacijama nije bila samo optimistična, već i neskladna s povijesti telekomunikacija. Ovo izvješće istražuje tu povijest i pokazuje kako su moć i telekomunikacije gotovo uvijek bile usko povezane. Kad su države ignorirale te veze i olako shvaćale sigurnost vlastitih mreža, rezultati su bili nepovoljni, a ponekad čak i pogubni.

Ovo izvješće proučava nekoliko glavnih slučaja natjecanja velikih sila u telekomunikacijama još od najranijih početaka elektroničkog sustava telekomunikacija u 1840-ima. Ti slučaji pokazuju da su mnoga pitanja s kojima se danas suočavaju kreatori politike slična onima iz prošlosti. Iako se sadašnja rasprava o mrežnoj sigurnosti i infrastrukturi tehnologije 5G može činiti novom, ona zapravo priziva zaboravljene sporove koje datiraju u prvim počecima elektroničkog sustava telekomunikacija prije otprilike 150 godina. Štoviše, mnogi poznati elementi telekomunikacijskog natjecanja danas, poput upotrebe organizacija za normizaciju, državnih subvencija, razdjelnika kabela, informacijskih operacija, tržišta zemalja u razvoju i šifriranja radi stjecanja prednosti, razvijeni su prije više od jednog stoljeća, s važnim poukama za sadašnje rasprave.

Popis tih ključnih pouka nalazi se u nastavku:

1. **Kontrola nad globalnim telekomunikacijskim mrežama oblik je političke moći.** Očekuje se da će mreže 5G stvoriti temelj pametnijem, povezanom gospodarstvu povezujući bezbroj uređaja i senzora. Nestrpljiva da izgradi ove mreže diljem svijeta, Kina je subvencionirala svoje tvrtke i projekte koji su prvaci tehnologije 5G diljem svijeta u sklopu inicijative „Digitalni put svile“. Taj je pokušaj nalik težnji Velike Britanije za dominacijom u mrežnoj infrastrukturi u prvim počecima električnog telegrafskog sustava. Velika Britanija svoju je prednost stvorila tijekom šest desetljeća postupnim povećanjem ovisnosti drugih država o svojim mrežama, čak i odustajanjem od naknada i ekonomskih koristi kako bi ih namamila da provedu kabele diljem Velike Britanije, istovremeno smanjujući britansku ovisnost o stranim mrežama. Kontrolirala je s vremenom više od polovice svjetske kabelske infrastrukture, najveću radijsku mrežu i

najveću flotu brodova za polaganje kabela. „Informacijska hegemonija“ Velike Britanije omogućila joj je da izbaci Njemačku iz gotovo svih globalnih telekomunikacija u Prvom svjetskom ratu i prisilila je Berlin da usmjeri promet preko linija u britanskom vlasništvu podložnih njezinom nadzoru, što se kasnije pokazalo presudnim u porazu Njemačke u sukobu.

2. **Duga razdoblja mira i prosperiteta uglavnom dovode do nezainteresiranosti za telekomunikacijske rizike.** U posljednjih 30 godina, mir i ekonomska globalizacija posthladnoratovskog razdoblja poklopili su se s brzim napretkom u telekomunikacijama koji je naveo države da prednost daju revolucionarnim komercijalnim koristima nad političkim i sigurnosnim rizicima, uključujući čak i strano vlasništvo ili upravljanje mrežama. Sličan se događaj odvio u ranim počecima telekomunikacija 1840-ih, što se također podudaralo s razdobljem relativnog mira i globalizacije koje se nastavilo sve do Prvog svjetskog rata. Veći je dio tog doba želja za dosezanjem naizgled čudesnog komercijalnog potencijala novih komunikacijskih tehnologija prikrivala pitanja vezana uz pouzdanost stranih mreža ili tvrtki. Velika je Britanija profitirala od tuđe nezainteresiranosti gradeći, a zatim i iskorištavajući neoboriv položaj čvorišta u globalnim mrežama, dok je većina drugih velikih sila ovisila o njezinim mrežama.

3. **Kad su države nezainteresirane za svoju telekomunikacijsku sigurnost, rezultati mogu biti pogubni i preoblikovati svjetsku politiku.** Desetljeća njemačke nezainteresiranosti o ovisnosti o britanskim telekomunikacijskim linijama značila su da je, dok je Berlin shvatio rizike te ovisnosti, bilo prekasno za promjenu. Kad je izbio Prvi svjetski rat, Velika Britanija presjekla je sve njemačke kabele i prisilila Berlin da usmjerava promet kroz britanske mreže usprkos riziku od presretanja, što je dovelo do otkrivanja „Zimmermanovog telegrama“ zbog čega su Sjedinjene Američke Države pristupile ratu. Slično tome, ruska neorganiziranost u bežičnim radijskim prijenosima u Prvom svjetskom ratu omogućila je Nijemcima da presretnu komunikacije, „uoče“ kretanje ruskih trupa u stvarnom vremenu i nanesu im odlučujući poraz u bitci kod Tannenberga. Zatim je u Drugom svjetskom ratu prekomjerno samopouzdanje nacista u vlastite šifre dovelo do minimalnih pokušaja da ih se ažurira, što je Velikoj Britaniji omogućilo razbijanje šifri i dobivanje obavještajnih podataka za koje se vjeruje da su skratili rat za dvije do četiri godine. S obzirom na moć informacija, čak i povremene pojave neorganiziranosti signalizacija ili nezainteresiranosti mogu promijeniti povijest.

4. **Nova tehnologija uvijek dovodi do novih pokušaja da je se presretne.** Pojava podmorskih kabela dovela je do pokušaja da se te linije presjeku i prisluškuju već u Španjolsko-američkom ratu; radijski prijenos iznjedrio je pokušaje protivnika da zauzmu mrežne čvorove i presretnu prijenose, a pojava sofisticiranih šifri za šifriranje proizvela je pokušaje industrijskih razmjera da ih razbiju. U svakom su dobu pojedini vjerovali da bi novi napredak u komunikaciji mogao biti manje ranjiv od onih koji su mu prethodili. Međutim, svaki se put nastavio ciklus inovacija i iskorištavanja.

5. **Telekomunikacijske mreže nikad nisu bile politički neutralne, posebno u vremenima napetosti.** Izvršni su se direktori tvrtke Huawei 2019. godine zavjetovali na

pristup „bez sigurnosnih rupa, bez špijuniranja“ i obećali da će njihova tvrtka ostati izvan politike, a kineska se vlada obvezala poštivati taj zavjet. No, čak i prije više od jednog stoljeća, telekomunikacijske tvrtke i njihove domaće vlade javno su davale slična obećanja, dok su ih privatno kršile i radile zajedno u razdobljima rata i mira. Na primjer, britanska dominacija podmorskim kabelima navela je Francuze, Nijemce i Amerikance da se zalažu za održavanje linija neutralnim, čak i u ratu. Britanske su tvrtke javno proglasile svoju neutralnost, ali zapravo su se priklonile britanskim političkim interesima, posebno u trenucima velikih napetosti, i u potpunosti se odrekle neutralnosti tijekom ratnih razdoblja. Moć koja dolazi od ometanja ili presretanja protivničkih protoka informacija općenito je bila previše primamljiva da bi je mogle podnijeti čak i iskrene tvrdnje o neutralnosti.

6. **Države često traže vlastite prvake u telekomunikacijama nakon što prepoznaju ranjivost oslanjanja na konkurentske ili protivničke tvrtke.** Sjedinjenim Američkim Državama trenutno nedostaje glavni proizvođač 5G baznih stanica, što je izazvalo rasprave o tome trebaju li ulagati u vlastite ili se oslanjati na suradničke tvrtke. To je također potaknulo neslaganje oko toga u kojoj je mjeri tvrtka Huawei sama po sebi de facto državni prvak. Ove rasprave imaju neki presedan. Početkom 20. stoljeća mnoge su države koje su se oslanjale na druge za telekomunikacijsku opremu ili mreže počele graditi vlastite sustave. Na primjer, Njemačka je potaknula dvije njemačke tvrtke Siemens & Halske i AEG s natjecateljskim radijskim pokušajima da zajedno uspostave njemačku alternativu britanskoj dominaciji u radiju. Mnoge druge vodeće države podržavale su tvrtke koje su se, premda su tobože bile privatne, ispreplele s državama koje su ih podržavale.

7. **Borba za telekomunikacijske standarde može odrediti koje će države imati mrežnu moć, a često zahtijeva angažiranje saveznika i partnera.** Države čija tehnologija postaje dominantan standard mogu imati tu prednost nad drugima. Trenutno natjecanje za standarde za informacijsko-komunikacijsku tehnologiju na ovaj je način slično anglo-njemačkom natjecanju za radijske mreže. Velika Britanija je putem tvrtke Marconi koju je podržavala bila toliko dominantna u području bežičnog radija da su sve ostale velike sile morale slati poruke preko britanske bežične mreže, koja je odbila uspostaviti vezu s bilo kojim drugim bežičnim stanicama. Njemačka je na kraju uspjela razbiti tu dominaciju s pomoću organizacije za normizaciju koja je zabranila ovu politiku „bez recipročne komunikacije“ uz pomoć drugih sila, uključujući Sjedinjene Američke Države i Francusku, što je prikaz načina na koji bi danas liberalne države mogle upotrebljavati slične koalicijske pristupe za postavljanje ili očuvanje povoljnih standarda za informacijsko-komunikacijsku tehnologiju (ICT) ako rade zajedno.

8. **Države se okreću šifriranju jer njihova komunikacija postaje lakša za presretanje, ali šifriranje često ima ograničenja zbog odlučnih protivnika ili korisničke pogreške.** Neki tvrde da je zabrinutost zbog uloge tvrtke Huawei u mrežnim tehnologijama ili zbog opće ranjivosti uređaja povezanih s internetom ublažena modernim šifriranjem. Ovakve tvrdnje imaju dugu povijest. U ranim počecima telekomunikacija prije jednog stoljeća, mogućnost da telegrafske poruke mogu čitati drugi koji kontroliraju mrežne čvorove ili da radio može presretati pasivna oprema za prisluškivanje, dovela je do velikog napretka

u šifriranju koji je rezultirao povremenim prekomjernim samopouzdanjem. Smatralo se da su njemački složeni strojevi s rotorima za šifriranje neprobojni, ali korisnička pogreška i britanski pokušaji industrijskih razmjera omogućili su Velikoj Britaniji da ugrozi njemačke šifre. Jeftine su nadogradnje njemačke opreme i šifri mogle okončati britansku prednost, ali prekomjerno samopouzdanje Berlina u šifriranju spriječilo je te promjene izdavanjem presretnutih obavještajnih podataka koji su preoblikovali tijek rata. Šifriranje „end-to-end“ znatno je naprednije od prethodnih pokušaja šifriranja, ali povijest nalaže da je potrebna određena poniznost.

9. **Mnoge države ne uzimaju u obzir razinu do koje protivnik može učiniti izvanredne napore da kompromitira njihove mreže.** Usred rasprava o modernim telekomunikacijama, vrijedno je napomenuti da su države koje su prednost davale jednostavnosti ili trgovini, a time i upotrebljavale sigurnosne prečace, često bile neugodno iznenađene pokušajima koje odlučni protivnik poduzima kako bi ugrozio njihove mreže. U Prvom je svjetskom ratu Njemačka bila iznenađena brzinom i nemilosrdnosti kojom je Velika Britanija presjekla sve kabele koje je Njemačka upotrebljavala za pristup vanjskom svijetu; slično tomu, ruski su zapovjednici bili iznenađeni kad je njihova neorganiziranost radijske mreže dovela do pogubnog poraza kod Tannenberga. U Drugom svjetskom ratu Njemačka nije očekivala da će Britanci razviti visoko centraliziranu operaciju razbijanja šifri industrijskih razmjera koja bi mogla iskoristiti njemačke komunikacijske pogreške, bez obzira na to bile one beznačajne ili prolazne, za razbijanje njemačkih šifri. I tijekom Hladnog rata, Sovjeti nikad nisu šifrirali unutarnju podvodnu telefonsku liniju za koju su vjerovali da je izvan dosega Sjedinjenih Američkih Država, ali je Washington unatoč tome pronašao način da je prisluškuje, stekavši tako neprocjenjiv izvor obavještajnih podataka.

10. **Kad je u pitanju sigurnost mreže, ne radi se samo o presretanju već i o napadima.** Neke od rasprava o ulozi tvrtke Huawei u mrežama naglašavaju pitanja sigurnosti podataka, ali njihova bi korist bila veća u razmatranju mrežnih napada, što je bio važan dio telekomunikacijskog natjecanja velikih sila. U ranim je počecima telegrafije bilo vidljivo kako velike sile pokušavaju presjeći kabele i uskratiti komunikacije, što je kulminiralo britanskom nečuvenom i dobro isplaniranom operacijom da presiječe sve kabele diljem svijeta koji bi mogli Njemačku povezati s vanjskim svijetom. Ponekad si država može naštetiti u provođenju strategija mrežnih napada, ali svejedno će nastaviti ako vjeruje da je šteta veća za njezinog protivnika.

Velike sile i telekomunikacije

„Velika su carstva uložila velik napor za ubrzanje protoka informacija“, bilježi jedna povijest telekomunikacija. „Rimljani su gradili ceste, Perzijanci i Mongoli održavali su utrke konja, Britanci su subvencionirali poštanske parobrode“.[2] No, iako su države žudjele za informacijama, njihov je protok ostao ograničen do pojave modernog telegrafa. Elektrifikacija protoka informacija stvorila je moderne telekomunikacije, a s time i poznate obrasce rivalstva velikih sila nad njima.

Ta prva desetljeća modernih telekomunikacija koja su trajala od 1840. do Prvog svjetskog rata dijele važne karakteristike s današnjicom. To je razdoblje, poput trenutnog posthladnoratovskog doba, bilo razdoblje relativnog mira velikih sila koje je vodeće države učinilo „manje osjetljivima“ po pitanjima politike i sigurnosti u telekomunikacijskim mrežama.[3] Dok su velike sile izgrađivale nacionalne i međunarodne mreže u 19. stoljeću, mnogi su se u početku zadovoljavali prepuštanjem vodstva industriji, ignoriranjem nacionalnosti privatnih tvrtki i umanjivanjem rizika protivnikove kontrole nad telekomunikacijskim mrežama. Koristi revolucionarnih promjena u telekomunikacijama, što su neki u to vrijeme nazivali „uništenjem vremena i prostora“[4], bile su toliko očite i zapanjujuće da se „vlasništvo nad kabelima smatralo manjim problemom“.[5] U telegrafiji se u tom razdoblju radilo više o poslu nego o politici, napominje jedan povjesničar u zapažanju koje se jednako lako moglo primijeniti na dio početnog uzbuđenja zbog moderne informacijske tehnologije i njezine najnovije inkarnacije: 5G.[6]

Razdoblje nezainteresiranosti velikih sila nije moglo potrajati. Države poput Perua 1879., a zatim Sjedinjenih Država 1898. bile su neke od prvih koje su presjekle telekomunikacijske mreže protivnika. Kako su napetosti velikih sila porasle, države diljem svijeta probudile su se i utvrdile da su neke od njih, većinom Velika Britanija, na dobar način održavale razdoblje mira i putem svojih privatnih tvrtki stekle monopol u međunarodnim komunikacijama.

Sve više uplašeni od ovisnosti o britanskim podmorskim kabelskim mrežama, države poput Francuske i Njemačke u velikoj su mjeri subvencionirale razvoj vlastitih mreža u razvoju koji se ne razlikuje od kineskog subvencioniranja i zaštite vlastitih prvaka u informacijskoj tehnologiji poput tvrtki Alibaba, Baidu, Tencent i Huawei. I kao što povjesničarka Heidi Tworek bilježi, protivnici Velike Britanije također su se kladili na sljedeću generaciju telekomunikacijske tehnologije – „bežičnu telegrafiju“, poznatiju kao radio – nadajući se da će smanjiti ovisnost o podmorskim telegrafskim kabelima u britanskom vlasništvu.[7] Iako su Britanci vodili na ovom polju, Njemačka se odbila pouzdati u britanske mreže. Izgradila je vlastitu mrežu s državnim prvacima koji prodiru u manje povezane dijelove svijeta, poput Latinske Amerike, Afrike i Azije, što bi danas moglo odražavati širenje kineskih tehnoloških tvrtki u svijet u razvoju i odlučnost Pekinga da postavi temelje za 5G mreže.

Kroz to su razdoblje države tog doba mnoge elemente telekomunikacijskog natjecanja velikih sila koje se danas zanemaruju često shvaćale prilično ozbiljno. Njemačka, frustrirana britanskom dominacijom u radijskim mrežama, upotrijebila je organizaciju za normizaciju kako bi slomila britansku dominaciju, a to predstavlja taktiku koja pokazuje da ta tijela nisu bila manje važna u to doba nego što su sada. A kako su telekomunikacije postajale bežične i još lakše presrestive, velike su sile polagale vjeru u šifriranje ponekad prije nego u organizirani rad svojih mreža pod

pretpostavkom da će „šifre“ (detaljni koraci za šifriranje ili dešifriranje poruka) riješiti problem; uvjerenje koje se gotovo uvijek pokazalo pogrešnim zbog korisničke pogreške. To gledište ima zapanjujuće poveznice s modernim pretpostavkama o općoj nesigurnosti telekomunikacijskih mreža i o uvjerenju koje su neki spominjali u raspravama o tvrtki Huawei da bi šifriranje u velikoj mjeri neutraliziralo rizik kineskog pristupa nečijoj telekomunikacijskoj mreži.

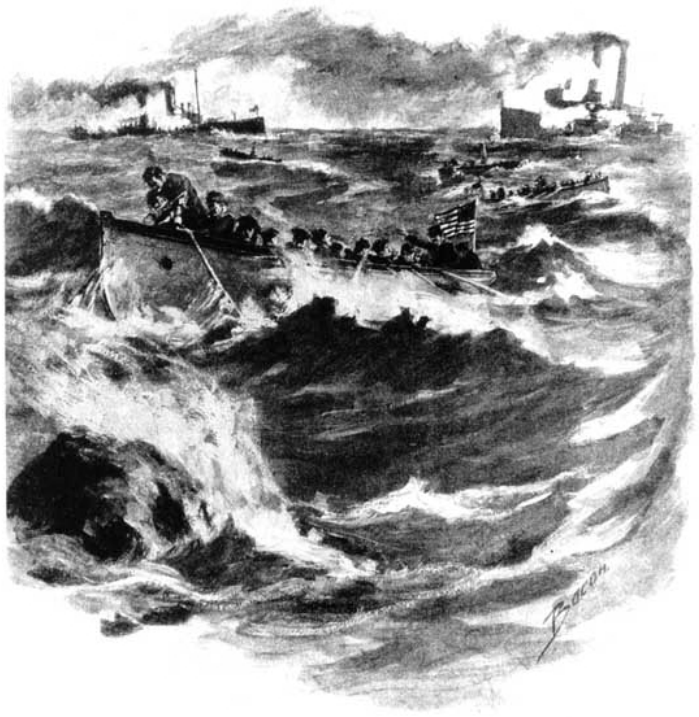
Kad je mir velikih sila završio i izbio rat, odjednom se očitovala politička važnost telekomunikacija koja u razdoblju mira nije bila uvijek jasna. Njemački uspjeh u presretanju ruskih prijenosa u Prvom svjetskom ratu donio je tako temeljitu pobjedu u bitci kod Tannenberga da je promijenio tijek rata i pomogao ubrzati izlazak Rusije iz sukoba. Britanska dominacija podmorskim kabelima u Prvom svjetskom ratu bila je toliko potpuna da je izbacila Njemačku iz globalnog telekomunikacijskog sustava, usmjerila njemački kabelski promet kroz vlastite mreže i na kraju otkrila Zimmermanov telegram, zbog čega su Sjedinjenje Američke Države pristupile ratu. U Drugom svjetskom ratu Velika Britanija postigla je još jedan obavještajni uspjeh razbijanjem njemačkih šifri za koje se smatralo da su neslomljive, što je dovelo do neusporedivih podataka za koje britanske službene povijesti tvrde da je skratio rat u Europi za nekoliko godina. Ti slučaji pokazuju da sigurnost telekomunikacija nije samo stvar taktike bojišta, već i političkog natjecanja, onog koja može diktirati sudbinu velikih sila i oblik svjetske povijesti.

Kako je svijet prisustvovao u američko-sovjetskom Hladnom ratu, britanske su prednosti smanjili ne samo američka snaga već i tehnološki pomaci koji su starije mreže učinili manje bitnima, pokazujući važnost da velike sile ostanu na vodećem položaju u tehnologiji. U tom se novom dobu telekomunikacijsko natjecanje nastavilo poznatim putem. Na primjer, Sjedinjene Američke Države bile su pionir novih načina prisluškivanja podmorskih kabela koji su bili zakopani toliko duboko i smatrani toliko sigurnima da poruke na njima često nisu bile šifrirane. Natjecanje se preselilo i u druge domene, poput satelita i internetske infrastrukture, iako se velik dio ove povijesti još uvijek piše i, u većini slučaja, ostaje tajan.

Kako pokazuje ovaj kratki niz slučaja, telekomunikacije su uvijek bile političke. Iskorištavanje ovih tehnologija i mogućnosti općenito je napredovalo zajedno s njihovim razvojem. Čim su stigle nove metode komunikacije, velike su sile uglavnom tražile načine da ih presretnu ili prekinu. „Električne komunikacije često su opisivane kao jedno od velikih dostignuća čovječanstva,“ napominje jedan povjesničar telekomunikacija, „ali kad to promatramo sa stajališta sigurnosti, vidimo sasvim drugu sliku jer sigurnost nije tehnička već socijalna i politička karakteristika.“ A „budući da se politika nije popravila“, napominje, „telekomunikacije imaju tamnu stranu.“[8]

Sad se okrećemo sažetku ključnih tema u gotovo dva stoljeća telekomunikacijskog natjecanja.

1. Španjolsko-američki rat: granice neutralnosti kabela



Prikaz američke ekspedicije presijecanja kabela u Cienfuegosu objavljen 1907. godine. Operacija je pokazala da čak ni velika sila koja je nekoć zagovarala neutralnost kabela neće tretirati podmorske telegrafske kabele kao neutralne tijekom oružanog sukoba.

Izvor: Naval Historical Center Online Library[9]

Kad su se podmorski kabeli počeli širiti uzduž cijelog svijeta u 19. stoljeću, nekoliko vodećih sila, uključujući Francusku, Njemačku i Sjedinjene Američke Države, zatražilo je da ih se izolira od međunarodne politike. U jednom od prvih ikad poslanih transatlantskih kabela, američki predsjednik James Buchanan 1858. godine pozvao je kraljicu Viktoriju da osigura da nove svjetske telegrafske linije budu „zauvijek neutralne... čak i usred neprijateljstava“.[10]

Kad su izbila neprijateljstva, napuštena su visoko nastrojena načela neutralnosti. Dva desetljeća nakon Buchananove poruke, Peru je presjekao čileanske kabelske vodove koji su se nalazili na spornom teritoriju.[11] Tom se sporu pridalo malo pažnje, ali kad su Sjedinjene Američke Države, nekadašnji prvak u neutralnosti kabela, presjekle kabele i u Atlantiku i u Tihom oceanu u španjolsko-američkom ratu, svijet je to primijetio.

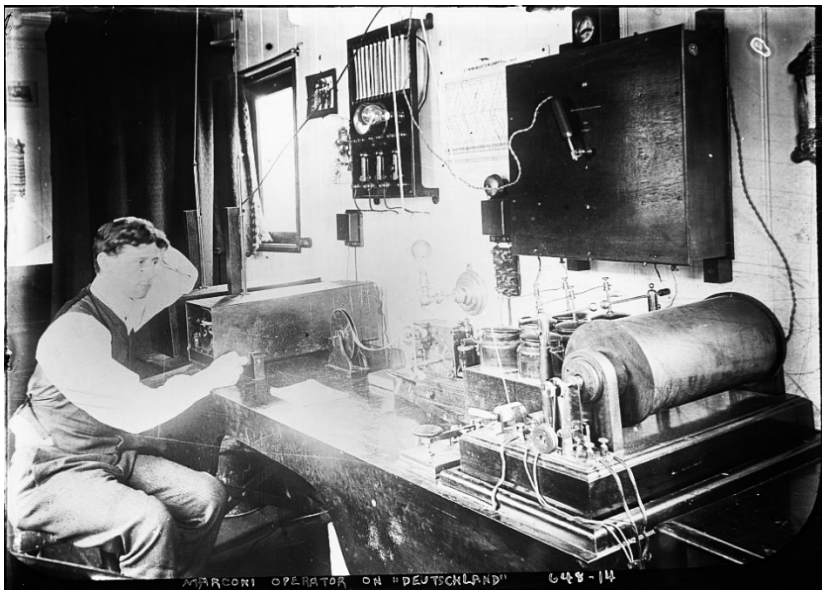
Američko presijecanje kabela planirano je prije sukoba. Sjedinjene Američke Države nadale su se da će u atlantskom bojištu odsjeći Španjolsku od njezinih snaga na Kubi. „Izolacija Havane bila je, naravno, od iznimne važnosti“, izjavio je tad jedan američki časopis i to je zahtijevalo da Sjedinjene Američke Države „isključe Havanu od svake telegrafske komunikacije s vanjskim svijetom“.[12] Sjedinjene Američke Države započele su s presijecanjem španjolskog prometa koji je prolazio kroz američki teritorij na Floridi. Zatim su poslale malu američku postrojbu da uništi

ključni telekomunikacijski čvor u Cienfuegosu, time odcijepljujući od Španjolske grad Havanu i veći dio zapadne Kube. Poslije su Sjedinjene Američke Države napale razne kabele na istoku Kube, kao i karipske kabele koji su Portoriko povezivali sa Španjolskom.[13] Rezanje kabela značajno je pogoršalo sposobnost Španjolske pri usmjeravanju i zapovijedanju snagama na Kubi.[14]

U Tihom su oceanu Sjedinjene Američke Države presjekle jedini podmorski kabel između Manile i Hong Konga, čime su Filipini odvojeni od Španjolske.[15] Odluka je naštetila i američkim komunikacijama, ali pretpostavljalo se da je Španjolskoj nametnuta još veća šteta, a Sjedinjene Američke Države mogle su to nadoknaditi redovitim otpremanjem jednog plovila u Hong Kong radi slanja dispečera natrag u Washington.[16] Američke su snage također presjekle podmorske kabele unutar Filipina, što je još više umanjilo sposobnost Španjolske da zapovijeda svojim snagama.

Španjolsko-američki rat bio je možda prvi globalni sukob na više bojišta u kojem su bile važne električne telekomunikacije. To je također označilo prvi put da je jedna velika sila nastojala zabraniti drugoj pristup podmorskim kabelima. Prije sukoba, telegrafija se još uvijek doživljavala kao prvenstveno komercijalno carstvo, a mnogi su se nadali da će kabeli ostati ograđeni od političkog i vojnog natjecanja. Sukob je dokazao ograničenja takvih perspektiva i pokazao da je kontrola nad telekomunikacijskom infrastrukturom i sposobnost uskraćivanja tih prednosti geopolitičkim protivnicima uvijek bila od kritičnog političkog značaja.

2. Anglo-njemačko rivalstvo: izgradnja mreža i postavljanje standarda



Radio operater tvrtke Marconi u „Marconijevoj sobi" njemačkog oceanskog broda SS Deutschland. Utjecaj tvrtke Marconi bio je toliko velik da su njihovi zaposlenici radili u njemačkim radijskim sobama iako je Njemačka bila zabrinuta zbog rizika od presretanja i mrežnih napada.

Izvor: Library of Congress, George Grantham Bain Collection[17]

Tehnološko postavljanje standarda i njegovi prateći mrežni učinci dugogodišnje su i suptilno poprište natjecanja velikih sila. Države čija tehnologija postaje dominantni standard mogu iskoristiti tu prednost nad drugima koja se ne gubi kod sila u usponu, koje često rade na smanjenju svoje ranjivosti stvaranjem paralelnih sustava. Doista, sadašnje kinesko-američko natjecanje oko informacijsko-komunikacijske tehnologije odražava stoljetno nadmetanje između Njemačke i Velike Britanije za dominaciju u informacijsko-komunikacijskoj tehnologiji (ICT) iz tog doba, s neobičnim paralelama i ključnim poukama za sadašnjost.

Krajem 19. stoljeća, talijanski inženjer Guglielmo Marconi, uz podršku Britanske kraljevske mornarice, stvorio je bežičnu telegrafiju.[18] Izum je bio revolucionaran. Iako su velike sile u prošlosti međusobno jedne drugima rezale kabele i dok je komunikacija od broda do broda i od broda do obale prije bila teška, Marconijev sustav riješio je te probleme i bio manje sklon smetnjama.[19] Marconi se na kraju udružio s Velikom Britanijom, omogućavajući zemlji monopol nad radio prijenosima. U kombinaciji s britanskim udjelom od 60 % u svjetskoj podmorskoj kabelskoj mreži, Velika Britanija dominirala je međunarodnim prijenosima. Britanska je prednost bila uznemirujuća za Njemačku, ali natjecanje za bežičnim tehnologijama također je „pružilo priliku Njemačkoj da izvrši kontrolu nad novom međunarodnom infrastrukturom" i da „zaobiđe britanske kabele", a primat velike sile bio je vezan za ishod.[20]

Osjećajući se ranjivim, Kaiser Wilhelm II odobrio je izravnu državnu potporu njemačkim znanstvenicima i inženjerima jer su uspješno kopirali Marconijeve nacrte, patentirali ih u

Njemačkoj i izgradili vlastite radijske mreže financirane ugovorima s njemačkom vojskom.[21] Unatoč tomu, Marconijeva prednost daljeg radijskog dometa i prednost kao prvog pokretača uspostavila je njegovu tvrtku s britanskom podrškom kao globalni standard, a Marconi je iskoristio ove mrežne učinke kako bi vodio politiku „bez recipročne komunikacije“ s radio operaterima koji nisu pripadali tvrtki Marconi. Njemačke tvrtke i oceanski brodovi nisu željeli biti odsječeni od globalne komunikacije, pa su više prihvaćali britanski sustav nego njemački.

Kaiser Wilhelm II pojačao je njemačku industrijsku politiku kako bi osporio britanski standard. Brzo je odredio da se dvije velike njemačke električne tvrtke Siemens & Halske i AEG s konkurentskim pokušajima vezanim uz radio udruže kako bi pružile definitivnu njemačku zamjenu naziva Telefunken. „[Domaće] rivalstvo na polju bežične telegrafije slabi konkurentnost Njemačke“, objasnio je Kaiser, „i daje tvrtki Marconi priliku da postigne svjetski monopol“ koji „nije bio u njemačkom interesu“.[22] Za vrijeme Kaisera Wilhelma II, Njemačka je vršila protekcionizam zabranjivanjem Marconijevih sustava u nekim slučajima. Pratila je tržišta u razvoju prodajom svoje tehnologije Južnoj Americi i Africi kako bi postavila standard u tim regijama i osigurala prihod.

Kad su se ti napori pokazali nedovoljnima, Njemačka je uspjeh ostvarila putem multilateralnim organizacijama za normizaciju. Njemačka je 1906. godine organizirala sastanak velikih sila na prvoj Međunarodnoj radiotelegrafskoj konvenciji, konferenciji o radio standardima. Tamo su članice zajednički zabranile Marconijevu politiku „bez recipročne komunikacije“, razbile britanski monopol i uspostavile djelotvoran anglo-njemački duopol.[23]

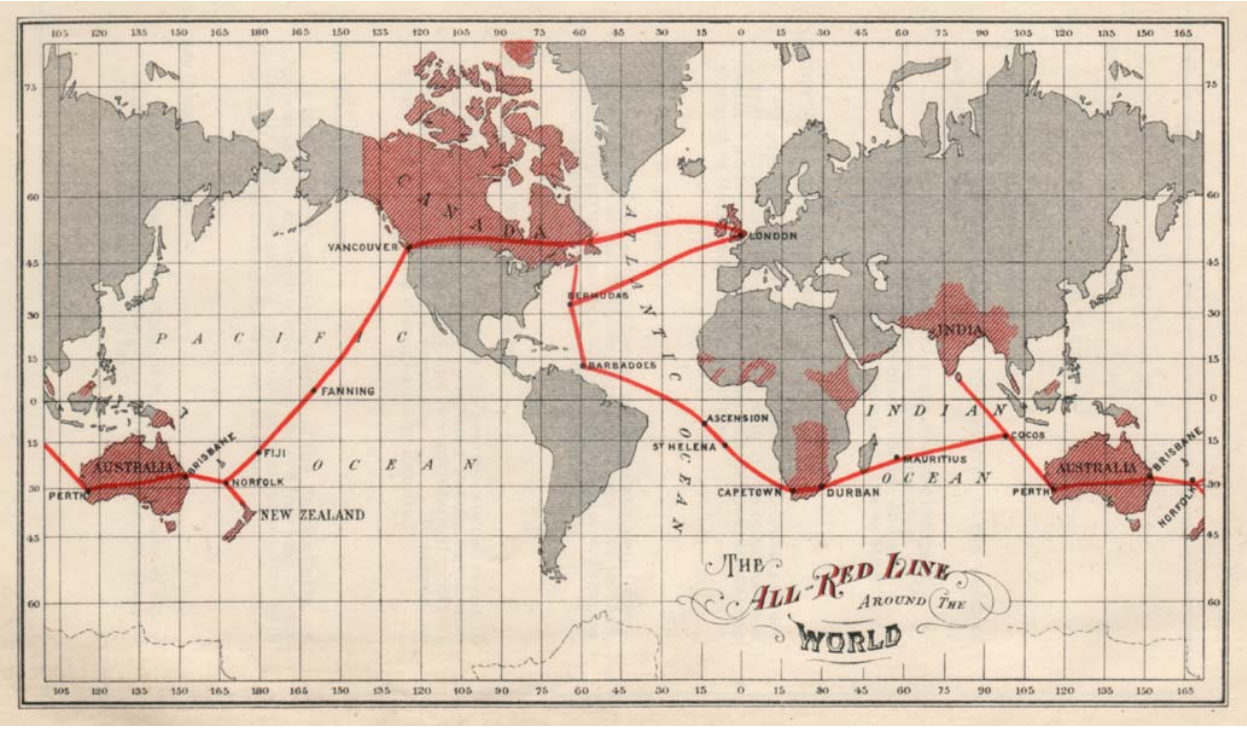
Anglo-njemačko natjecanje otkriva da organizacije za normizaciju imaju ogromne strateške implikacije. Kina danas upotrebljava mnoge tehnike koje je Njemačka upotrebljavala prije jednog stoljeća, poput državne industrijske politike, državne zaštite, izdašnih državnih ugovora, civilno-vojne integracije, zabrane konkurentskih proizvoda, prisilnih spajanja, potrage za tržištima u nastajanju, pa čak i međunarodnih ugovora za postavljanje standarda, što je sve pomoglo kineskim tehnološkim tvrtkama poput Alibabe i Tencenta, vlasnicima aplikacija WeChat i AliPay, da postanu lokalni prvaci. Te su se tvrtke od tada proširile u inozemstvo, često ne ciljajući američko tržište već, poput njemačke tvrtke Telefunken prije njih, nova tržišta s nižom dobiti i smanjenom konkurencijom.[24]

Kina također osporava standarde u izgrađenoj infrastrukturi internetske povezanosti. Njezina vlada ulaže milijarde kako bi kineski proizvođači čipova mogli pobijediti američke protivnike u utrci za standarde 5G mobilnog interneta. Slično tome, kineske tvrtke poput tvrtke Huawei i ZTE dobivaju državne zajmove za izgradnju infrastrukture internetske povezanosti u cijelom svijetu u razvoju. Kao što pokazuje britanski primjer, ti pokušaji ne samo da kinesku tehnologiju čine standardom, već nude i mogućnosti nadzora. U međuvremenu, inicijativa „jedan pojas, jedan put“ postavlja mogućnost Kini da postavi standarde za „pametnu infrastrukturu“ diljem Azije, posebno potrebne senzore i softvere te da drugim tvrtkama uskrati interoperabilnost, čime će ih isključiti iz industrije samostalnih vozila i drugih.

Anglo-njemačko rivalstvo u telegrafiji pokazuje da Washington mora ozbiljno shvatiti kineski državni izazov u standardima. To također nudi put naprijed. Na sličan način na koji je Njemačka upotrebljavala međunarodne konferencije da bi prekinula britanski monopol u telegrafiji,

Sjedinjene Američke Države mogle bi uspostaviti ili sačuvati povoljne standarde za informacijsko-komunikacijsku tehnologiju putem multilateralnih sporazuma. To bi moglo spriječiti Kinu od postavljanja unilateralne normizacije putem njezinih sporazuma o slobodnoj trgovini, državnih prvaka ili infrastrukturnih projekata.

3. Velika Britanija u Prvom svjetskom ratu: uvođenje hegemonije informacija



„All Red Line", skupa mreža britanskih podmorskih kabelskih vodova izgrađena s ogromnom zalihosti i uređena tako da nijedan dio nije prolazio teritorijem protivnika. Neadekvatno ulaganje Njemačke u vlastitu otpornu globalnu telekomunikacijsku mrežu omogućilo je Velikoj Britaniji da je odsječe od globalnih komunikacija, dok je Britanija bila bez posljedica.

Izvor: George Johnson, ed., The All Red Line: The Annals and Aims of the Pacific Cable Project / Internet Archive[25]

Pokušaji Njemačke da prekine britansku dominaciju u telekomunikacijama početkom 20. stoljeća nisu nastali iz paranoje. Nakon što je izbio Prvi svjetski rat, Velika Britanija uspješno je iskoristila svoj značajan utjecaj u telekomunikacijskim mrežama kako bi oblikovala tijek rata. Prerezala je njemačke kabele, nadzirala njemački prijenos i prisilila njemački promet u područje mreža pod britanskom kontrolom otkrivajući Zimmermanov telegram, zbog čega su Sjedinjenje Države pristupile ratu.[26]

Velika Britanija nije prva velika sila koja je presjekla ili manipulirala telekomunikacijskim mrežama: Peru je prekinuo vezu Čile – Bolivija, Sjedinjene Američke Države španjolske kabele, a Velika Britanija je u jednoj kriznoj situaciji ogradila Bure od svojih europskih pristaša, a u drugoj manipulirala kabelskim prometom prema Francuskoj.[27] Ali ti su pokušaji u Prvom svjetskom ratu išli do krajnjih granica.

Velika Britanija prva je odsjekla čitavu zemlju od glavnih globalnih telekomunikacijskih mreža, uvođenjem prvog dana rata plan koji je pažljivo sastavljen tijekom razdoblja mira.[28] U roku od godinu dana, Velika Britanija uništila je njemačke kabele diljem svijeta: u La Mancheu,

Sjevernom moru, Sjevernom Atlantiku, Južnoj Americi, većem dijelu Afrike, Dalekom Istoku, pa čak i u neutralnim zemljama koje su bile domaćini njemačke infrastrukture.[29]

Da bi to nadoknadila, Njemačka je pokušala proširiti radijsku mrežu koju je tvrtka Telefunken izgradila desetljeće ranije u Latinskoj Americi i na „Globalnom jugu" tako da pokriva svijet. U pokušaju s modernim usporedbama s kineskom inicijativom „digitalni put svile", Berlin je ponudio zajmove i ulaganja vladama zainteresiranim za „razvojne koristi od radija" kako bi bili domaćini njemačkih komunikacijskih čvorova. Kao odgovor, Velika Britanija nagovorila je ili potaknula većinu tih zemalja da se odreknu potpore njemačkim radio čvorovima ili ih je aktivno sabotirala.[30]

Ostavši bez vlastitih mreža, Berlin nije imao izbora nego oslanjati se na britansku mrežu tijekom rata. Na početku su Britanci počeli potiho nadzirati sav promet koji je prolazio kroz njihove kabele i iskoristili su tu prednost za vođenje informacijskih operacija protiv Njemačke, selektivno propuštajući neugodan njemački promet kako bi naštetili njenim odnosima s neutralnim zemljama. Kad je Njemačka poslala zloglasni Zimmermanov telegram predlažući vojni savez s Meksikom protiv Sjedinjenih Američkih Država, poruka je prošla kroz britansku mrežu, a presrela ju je i dešifrirala Velika Britanija koja ju je potom podijelila s vladom Sjedinjenih Američkih Država, a koja je zauzvrat podijelila to s američkom javnošću.[31] Taj je incident pomogao ulasku Sjedinjenih Država u rat, oblikovao svjetsku povijest i na kraju zapečatio poraz Njemačke.

Britanske informacijske operacije protiv Njemačke otkrivaju opasnosti pružanja protivničkoj sili mogućnosti nadzora nečijeg prometa ili isključivanja nečijeg telekomunikacijskog pristupa. Također otkrivaju da se mreže koje velike sile uzimaju zdravo za gotovo u razdoblju mira često u ratu napadaju i da će borba za komunikacijske čvorove neizbježno uključivati treće strane i neutralne zemlje.

4. Njemačka pobjeda u bitci kod Tannenberga: opasnosti od presretanja

Njemačka bežična terenska telegrafska stanica tijekom Prvog svjetskog rata. Nesposobnost Rusije da na odgovarajući način šifrira svoje komunikacije na svojim terenskim postajama dovela je do katastrofalnog poraza koji je preoblikovao tijek rata.

Izvor: C. O. Nordensvan and Valdemar Langlet, Det stora världskriget *[The Great World War]*[32]

Njemačka nije bila potpuno onesposobljena tijekom informacijskih operacija. Prerezala je ruske kopnene i podmorske kabele koji su je povezivali sa zapadnim saveznicima, kao i nekoliko transatlantskih kabela na koje su se oslanjali Britanci, te pokrenula upotrebu podmornica za ove zadatke.[33] S obzirom na zalihost britanskih mreža, ovi su pokušaji u konačnici bili manje iscrpljujući nego što su se Nijemci nadali. Ono što je prouzročilo više posljedica je njemačka upotreba radijskih obavještajnih podataka protiv Rusije tijekom bitke kod Tannenberga u kolovozu 1914. u prvom mjesecu rata, što je potaknulo katastrofalan poraz Rusa. Jedan njemački obavještajni časnik u to je vrijeme incident nazvao „prvim u povijesti ljudskog roda u kojem je presretanje neprijateljskog radio prometa odigralo presudnu ulogu“.[34]

Bitka se odvila usred ruskih dobitaka na istočnom frontu. Kako je Rusija zalazila dublje u Istočnu Prusku, njezina je vojska naišla na značajan komunikacijski izazov koji je stvorio povod za katastrofalan poraz. Nijemci u povlačenju presjekli su vlastite telegrafske linije, a Rusima koji su napredovali nedostajalo je dovoljno obučenog osoblja da uspostavi žičane komunikacije preko njihove rasprostranjene formacije. Radio prijenos bio je alternativa, ali iako su Rusi usvojili nove radio tehnologije za svoje vojno zapovjedništvo i kontrolu, nisu ih osigurali na odgovarajući način. Različitim skupinama dodijeljene su različite šifre; većina je imala malo iskustva s kodiranjem i dekodiranjem signala, a znalo se da su Britanci razbili neke šifre i knjige sa šiframa bile su ograničene ili nerazumljive za mnoge nepismene novake.[35] Rezultat je bio da su ruski zapovjednici smatrali da moraju riskirati upotrebom nešifriranih radio poruka i nadati se da ih Nijemci ne nadziru pažljivo.

Nijemci su, međutim, pomno pratili signale. Promatrajući rusku radijsku neorganiziranost u ratu protiv Japanaca, znali su da ruski nešifrirani prijenosi nisu dio kampanje obmane. Tako su upotrijebili svoje znanje o ruskim komunikacijama u stvarnom vremenu kako bi podigli „maglu rata“ i odlučno porazili nadmoćnu silu. Rusija je izgubila cijelu vojsku, s preko 100 000 žrtava i 92 000 zarobljenih u usporedbi sa samo 13 000 njemačkih žrtava.

5. Velika Britanija u Drugom svjetskom ratu: granice šifriranja

Mehanički rotori Lorenzovog stroja za šifriranje smatrani su učinkovito neslomljivima tijekom Drugog svjetskog rata. Britanski pokušaji da razbiju šifru omogućili su službenicima pristup njemačkoj komunikaciji na visokoj razini.

Izvor: Matt Crypto / Wikimedia Commons[36]

Izumi bežične telegrafije i radija donijeli su veću praktičnost u odnosu na fizičke kabele, ali su nosili veći rizik od presretanja. U Prvom i Drugom svjetskom ratu velike su sile djelovale u svijetu u kojem se pretpostavljalo da su radio komunikacije dostupne drugima. I u takvom se svijetu, koji se ne razlikuje od sadašnjih pretpostavki o ranjivosti modernih računalnih i telekomunikacijskih sustava, šifriranje smatralo ključnim za sigurnost. Rezultat je, kako je rekao jedan američki vojni povjesničar, bila „borba između kriptografa i kriptoanalitičara“.[37] Kad su velike sile bile na pogrešnoj strani te borbe, rezultati su mogli biti katastrofalni.

Da bi spriječile takav ishod, organizacije bi upotrebljavale šifre kako bi smanjile rizik da presretanje ugrozi sigurnost. Također su primjenjivali „organizaciju tijekom radio komunikacije“ kako bi spriječili protivnike da kroz analizu radio prometa steknu uvid u obrasce upotrebe.

Većina velikih sila uložila je u istinski industrijski napor kako bi proučila protivnički promet i, ako je moguće, razbila protivničke šifre. Velika Britanija bila je daleko centraliziranija u analizi protivničkih šifri od Njemačke koja je te funkcije proširila među nekoliko agencija. I kao što su britanski uspjesi u obavještajnoj singalizaciji i kriptoanalizi oblikovali tijek Prvog svjetskog rata, tako su oblikovali i tijek Drugog svjetskog rata kad je britanska operacija u centru Bletchley Park razbila njemačke šifre Enigma i Lorenz.

Sustavi šifriranja Enigma i Lorenz upotrebljavali su izuzetno složene rotorske strojeve za šifriranje poruka za koje je Njemačka vjerovala da neće „biti ranjive“.[38] Svako bi pritiskanje tipke zamijenilo znak drugim znakom na temelju jedinstvenih postavki stroja, a te postavke, koje su za Lorenzov sustav premašivale ukupan broj atoma u svemiru, pošiljatelj i primatelj trebali bi podijeliti da bi pročitali poruku.[39] Sustav Enigma upotrebljavali su vojska, Gestapo i diplomati, a sustav Lorenz, koji je bio još složeniji, Adolf Hitler i visoki nacistički te vojni dužnosnici upotrebljavali su za međusobnu komunikaciju.

Britanski uspjeh u razbijanju sustava Enigma i Lorenz rezultat je nekoliko događaja. Prvo, to je bio rezultat savezničke obavještajne suradnje s Poljskom, koja je iskoristila neke njemačke pogreške kako bi otkrila neke jednostavnije strojeve sustava Enigma.[40] Kao što je jedan britanski kriptoanalitičar tog vremena izjavio, njihov pokušaj „nikada ne bi uspio“ bez poljskih doprinosa.[41]

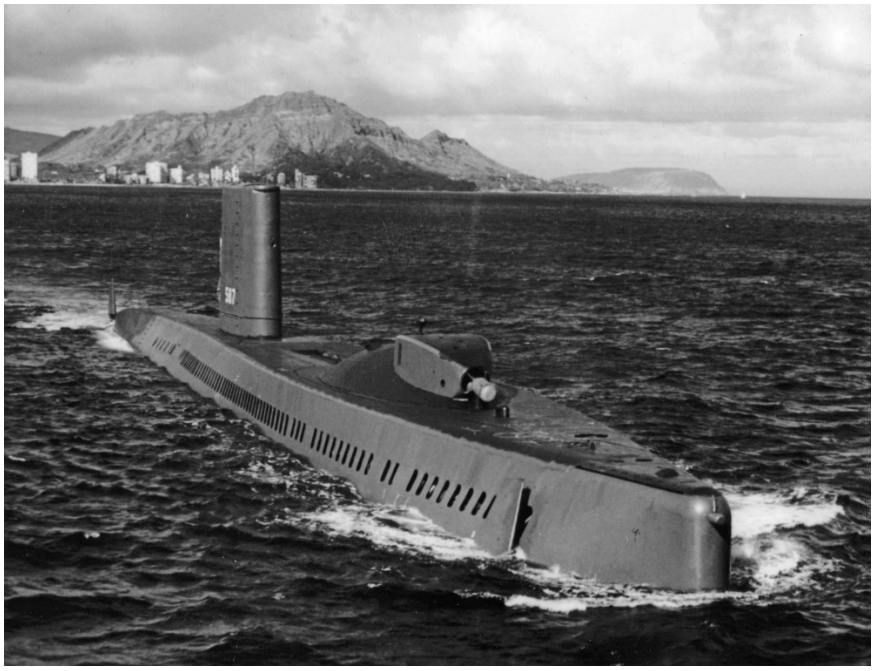
Drugo, bio je to proizvod njemačkog prekomjernog samopouzdanja, s tim da Njemačka nikad nije sumnjala da su šifre otkrivene i stoga je podlijegala prilično laganim preinakama koje su Veliku Britaniju prisilile da krene od početka.[42] Unatoč tome, njemačka vjera u neranjivost svojih strojeva „bila je gotovo ispravna“, ispričao je jedan visoki dužnosnik centra Bletchley Park.[43]

Konačno, rezultat jednog, ali velikog promašaja u njemačkoj „organiziranosti tijekom radio komunikacije“ stvorio je mogućnost za obrtanje njemačkih sustava šifriranja, iako ih nikad nisu uživo vidjeli.[44] Čak su i najsofisticiraniji sustavi bili osjetljivi na korisničke pogreške, a oprezan ih je protivnik mogao iskoristiti.

Razbijanjem sustava Enigma i Lorenz, Velika Britanija imala je pristup nekim najosjetljivijim komunikacijama Njemačke. Winston Churchill navodno je obavještajnim podacima pripisao ključan razlog zašto je Velika Britanija pobijedila u ratu, a Dwight D. Eisenhower navodno ih je nazvao „odlučujućim“.[45] Službeni povjesničar britanske obavještajne službe, Sir Francis Harry Hinsely, tvrdi da su ti uspjesi „skratili rat za ne manje od dvije godine, a vjerojatno i za četiri godine“, sabotirajući feldmaršala Erwina Rommela u Africi, naglo preokrenuvši savezničke gubitke u brodarstvu prema njemačkim podmornicama i omogućivši iskrcavanje u Normandiji.[46] Također su dopustili Velikoj Britaniji da identificira gotovo sve njemačke špijune koji ulaze u zemlju i često ih preobrate ili upotrijebe za prosljeđivanje neispravnih obavještajnih podataka, pri čemu je voditelj programa napomenuo da su britanske obavještajne službe „aktivno vodile i kontrolirale njemački špijunski sustav u ovoj zemlji“.[47] Malo je zemalja ikad imalo tako povjerljivo znanje o drugoj tijekom rata.

Zajedno uspjesi britanskih pokušaja protiv Njemačke, poljsko praćenje njemačkih komunikacija za vrijeme razdoblja mira i odluka da svoje otkriće podijeli s Velikom Britanijom imaju pouke primjenjive na današnje vrijeme kad velike sile provode kibernetičko izviđanje jedna protiv druge. Šire gledano, oni koji predlažu da šifriranje ublažava problematiku protivnikovog pristupa nekoj telekomunikacijskoj mreži možda čine pogrešku koja se ne razlikuje od one koju je sama Njemačka jednom učinila: pretjerana vjera u tehnologiju i ograničena pažnja na uvijek prisutnu mogućnost ljudske pogreške.

6. Operacija Ivy Bells: detalji potraga za informacijama



USS Halibut koji je navodno bio uključen u pokušaj prisluškivanja podmorske sovjetske telefonske linije.

Izvor: U.S. Navy / Wikimedia Commons[48]

Sovjetski Savez bio je mnogo oprezniji sa svojim šifriranjem nego što su to bili nacisti, oslanjajući se na vlastitu verziju sustava Enigma, poznatog kao Fialka, koji je bio znatno složeniji.[49] Iz tog razloga nepresušne riznice obavještajnih podataka na strateškoj razini proizvedene u Drugom svjetskom ratu nakon razbijanja njemačkih šifri nisu imale javno poznatu sličnost u Hladnom ratu. S obzirom na ove izazove, uvedene su i druge metode probijanja protivničkih telekomunikacija. Jedan od najsmjelijih pokušaja dogodio se u odnosu na podmorske kabele.

Početak podmorskih kabela u 19. stoljeću je na kraju doveo do pokušaja da ih se presiječe i povremeno prisluškuje, često u plićim vodama ili na kopnu gdje je takve zadatke bilo lakše izvesti. Suprotno tome, izvođenje ovih operacija u dubokim vodama pod nadzorom neprijatelja smatralo se gotovo nemogućim, pogotovo ako se to mora izvoditi tajno. Početkom 20. stoljeća, britanske, a potom i sukcesivne velike sile, došle su do odluke o podmorskoj sigurnosti kabela: ako su mjesta za iskrcavanje osigurana, a kabeli ne prelaze neutralne ili neprijateljske zemlje, tad bi općenito bili sigurni od presretanja i često sigurni od rezanja, posebno u razdoblju mira.[50]

Međutim, tijekom hladnog rata ta se računica promijenila. Pojava nuklearnih podmornica stvorila je mogućnost prisluškivanja podmorskih kabela u dubljoj vodi. No, smatralo se da je zadatak slanja ronilaca da pristupe kabelima na dubokom dnu mora sličniji istraživanju svemira nego poznatim pokušajima manipulacije kabelima koji su se pokušavali u prethodnim razdobljima. Stvaranje aparata za prisluškivanje koji bi se mogao postaviti u takvim uvjetima bilo je i tehnički zahtjevno.

Kad su Sjedinjene Američke Države sumnjale da bi sovjetski podmorski kabel mogao ići od pomorskog sjedišta u Vladivostoku do podmorske baze na poluotoku Kamčatki, pokušali su prevladati ove prepreke, iskazujući vrijednost signalnih obavještajnih podataka.[51] Vjerovalo se da će prisluškivanje tog snopa žica od pet inča pružiti kritične informacije o sovjetskim nuklearnim snagama.[52] Iako su Sovjeti šifrirali sav promet poslan zrakom, Sjedinjene Američke Države očekivale su da će Sovjeti pretpostaviti da je prometu zaštićenim podmorskim kabelom praktički nemoguće pristupiti, pa ga stoga neće šifrirati. Štoviše, „sovjetski admirali i generali bili su previše oholi i nestrpljivi da trpe gomilu kriptografa koji su već prenatrpani golemim teretom svog rada“, i inzistirali su na nesigurnim glasovnim komunikacijama.[53] Prisluškivanje bi tad pružilo malu količinu obavještajnih podataka, pa je američka mornarica pokrenula operaciju Ivy Bells kako bi to uspostavila.

Mnogo toga o prisluškivanju i obavještajnim podacima stečenim tim putem i dalje je povjerljivo, ali otvoreni izvori pružaju neke detalje o jedinstvenoj i inovativnoj operaciji. Sjedinjene Američke Države poslale su nuklearnu podmornicu USS Halibut, da oprezno prođe pokraj sovjetske mornarice i pronađe podmorski kabel na površini od 600 000 četvornih kilometara.[54] Inovativna tehnologija stvorena je kako bi se osiguralo da ronioci mogu raditi pod velikim pritiskom i na ekstremno hladnim temperaturama tijekom nekoliko sati. Slično tome, osmišljene su nove metode za postavljanje aparata za prisluškivanje u ovom izazovnom okruženju.[55] Sve je to trebalo učiniti bez ikakvog sovjetskog otkrivanja ili sumnje. Kad bi se brod otkrio, Sovjeti bi se na njega mogli ukrcati ili uništiti ga.

Operacija se na kraju pokazala uspješnom, a tijekom sedamdesetih godina američka mornarica prisluškivala je i snimala nezaštićene poruke preko kabela. Svakih nekoliko mjeseci američke bi se podmornice tiho šuljale sovjetskim vodama, izbjegavale napadačke podmornice, slale ronioce do prislušnih kabelskih vodova i dohvaćale vrpce sovjetske komunikacije koje su pružale izuzetno vrijedne i rijetke djeliće obavještajnih podataka. Iako su Sjedinjene Američke Države proširile „mrežu špijunskih satelita, zrakoplova, stanica za prisluškivanje i podmornica“ kako bi prikupile obavještajne podatke o signalima, „nisu mogle prodrijeti u žičanu telefonsku liniju“ na teritoriju protivnika. Ovaj je pokušaj ilustrirao evolucijski pomak u telekomunikacijama, većinom da odlučni akter s pravom tehnologijom može pristupiti podacima i signalima koji se prenose putem bilo kojeg medija i na bilo koji način. Iako je to prisluškivanje na kraju ugroženo izdajom, posljedično presretanje telekomunikacija pružilo je neprocjenjive vojne i političke obavještajne podatke Sjedinjenim Državama i njihovim saveznicima.[56]

Suvremeno natjecanje telekomunikacija u povijesnoj perspektivi

Do kraja Hladnog rata Sjedinjene Američke Države očito su zamijenile Veliku Britaniju kao hegemona informacija. Sjedinjene Američke Države zadržale su ključnu poziciju što se tiče globalnog interneta, stabilne mogućnosti u svemiru, dominacije u većini internetskih tehnologija i, prema javnim otkrićima, sofisticirane sposobnosti presretanja ili eventualnog napada neprijateljske komunikacije.

Te se američke prednosti sada ispituju, kao i britanske prije više od jednog stoljeća. Rusija, a posebno Kina, sad izazivaju američku dominaciju. Iako Sjedinjene Države uživaju ključnu poziciju u mnogim protocima podataka, druge sile sve više nastoje smanjiti svoju ovisnost o američkim mrežama. Istodobno, ključna američka pozicija manje je potrebna za presretanje nego što je britanska bila prije jednog stoljeća. Internet omogućuje upad bez kontrole nad fizičkom infrastrukturom. Pametni telefoni i računalne mreže mogu se hakirati, a jesu li nečije osjetljive komunikacije ugrožene fizičkim prisluškivanjem iz ranijeg doba ili virtualnim upadima modernog doba, krajnji rezultat je isti. Ovakva veza vjerojatno stvara veću ranjivost sad nego u doba telegrafa ili bežičnog radija.

Rusija je bila vodeća država u iskorištavanju te ranjivosti. Rusija je 2007. pokrenula val kibernetičkih napada na estonske organizacije, uglavnom distribuirajući napade uskraćivanjem usluga.[57] Godine 2008. pokrenula je kibernetičke napade u rusko-gruzijskom ratu. Uključeni su bili ne samo usmjereni napadi uskraćivanja usluge, već i pokušaji preusmjeravanja vladinih web-mjesta, preuzimanje gruzijskih vladinih poslužitelja i preusmjeravanje gruzijskog internetskog prometa putem poslužitelja pod ruskom kontrolom, s tim da su neki napadi izvedeni prije sukoba kako bi se poklapali s ruskom vojnom operacijom.[58] Prilikom napada Krima 2014. godine, Rusija je kombinirala kibernetičke napade s fizičkom kontrolom telekomunikacijskih mreža. Ruski su vojnici zauzeli ukrajinske telekomunikacijske objekte, upotrebljavajući ih za prekid komunikacije na Krimu, pa čak i za izvršavanje kibernetičkih napada i remećenja u drugim dijelovima Ukrajine.[59] Rusija je 2015. započela val kibernetičkih napada na ukrajinsku infrastrukturu, u dva bitna trenutka isključila je napajanje za stotine tisuća Ukrajinaca. Tijekom sljedećih nekoliko godina pokrenula je val napada bez presedana diljem Ukrajine koji se širio na „medije, financije, promet, vojsku, politiku i energiju“, gotovo svaki segment ukrajinskog društva, za što su neki vjerovali da je djelomičan pokušaj obuke za sličnu kampanju protiv Sjedinjenih Američkih Država.[60] Istodobno je nastavila niz napada diljem Baltika i slavno je nastojala oblikovati američke izbore 2016. i 2020. kampanjama dezinformacija, kao i u drugim zemljama.[61] Američka je vlada 2021. godine službeno optužila Rusiju za hakiranje IT tvrtke SolarWinds, sofisticirani napad koji je kompromitirao veći dio savezne vlade i nekoliko glavnih američkih tvrtki.[62]

Kina je druga glavna sila koja značajno ulaže u telekomunikacijsko natjecanje, iako za razliku od Rusije, Kina ne želi samo iskoristiti postojeću internetsku infrastrukturu već i izgraditi mreže i infrastrukturu na koju može utjecati, pa čak i kontrolirati. Poput Rusije, Kina je bila vješta u iskorištavanju postojećih internetskih ranjivosti. Početkom 2000-ih pokrenula je val napada na mreže Ministarstva obrane SAD-a što je Ministarstvo nazvalo Operacija Titan Rain.[63] Vlade diljem svijeta poput Sjedinjenih Američkih Država, Ujedinjenog Kraljevstva, Francuske, Njemačke, Kanade, Australije, Japana, Južne Koreje, Tajvana, Indije i preko desetak drugih,

žalile su se na kineski upad u njihove vladine mreže. Američki državni odvjetnik William Barr potvrdio je da su neke od najvećih kibernetičkih napada u posljednjem desetljeću počinili kineski agenti, uključujući krađe evidencija iz američkog Ureda za upravljanje osobljem (evidencija za 21 milijun ljudi), hotela Marriott (za 400 milijuna), tvrtki zdravstvenog osiguranja Anthem (za 80 milijuna) i Equifax (za 147 milijuna), između ostalih.[64]

Istovremeno, Kina također postavlja temelje za buduću internetsku infrastrukturu i, u svjetlu njezinih prethodnih pokušaja, malo je vjerojatno da je taj pokušaj sad komercijalan ili će ostati isključivo komercijalan u razdoblju koje slijedi. Kineska ulaganja najizraženija su u 5G mrežama za koje se očekuje da će stvoriti temelj za pametnije, povezano gospodarstvo koje povezuje bezbroj uređaja i senzora. Željna izgradnje ovih mreža diljem svijeta, Kina je subvencionirala svoje 5G prvake i projekte diljem svijeta kao dio inicijative „digitalni put svile“. Konkurentnim cijenama, tvrtke poput tvrtke Huawei uspjele su nadmašiti druge glavne dobavljače 5G i zavladati značajnim globalnim tržišnim udjelom, čineći Kinu liderom u izgradnji tih mreža. I osim 5G mreže, kineska je vlada subvencionirala pokušaje izgradnje internetske ili komunikacijske infrastrukture na gotovo svim kontinentima. Svi se pokušaji nadopunjuju kampanjom za oblikovanje globalnih standarda, ključnog prioriteta politike za Kinu ugrađenog u planske dokumente koji bi, kao u anglo-njemačkom rivalstvu oko radija prije jednog stoljeća, mogli oblikovati budućnost telekomunikacija na načine koji prednost daju Kini. U tu svrhu Kina je nedavno predstavila novu inicijativu za zaštitu podataka.[65]

Neki strahuju da kineske aktivnosti ostavljaju otvorenu mogućnost da će Peking imati de facto kontrolu nad tim mrežama, bilo da presretne promet ili uskraćuje pristup. O pokušajima Kine da stekne tu kontrolu dostupno je malo javnih podataka, ali američka je vlada u veljači 2020. otkrila da je tvrtka Huawei imala „sigurnosne rupe“ u svojoj mrežnoj opremi, nije ih otkrila relevantnim tvrtkama s kojima je sklapala ugovore i da su sigurnosne rupe prevazišle one koje ponekad zahtijevaju vlade domaćina kao dio zakonitih presretnutih razgovora.[66] Štoviše, javno izvještavanje otkrilo je da je tvrtka Huawei pomogla vladama zemalja poput Ugande i Zambije u kompromitiranju identiteta neistomišljenika.[67] Čak i nakon slučaja tvrtke Huawei, tvrtka za kibernetsku sigurnost nedavno je otkrila sigurnosne rupe u obveznom poreznom softveru koji kineska vlada zahtijeva od stranih tvrtki da ga instaliraju.[68] Bez obzira na to sugeriraju li ovi slučaji da je tvrtka Huawei i sama iskoristila svoj položaj u tim mrežama, ponašanje tvrtke i evidencije o Kini u kibernetičkim napadima i špijunaži razlog su za zabrinutost.

Drugi glavni razlog za zabrinutost dolazi iz povijesti i ponašanja čak i liberalnih velikih sila temeljitije ograničenih vladavinom zakona. Doista, prethodni povijesni slučaji izričito sugeriraju da će kineska vlada vjerojatno iskoristiti vrstu moći i utjecaja koju će imati tvrtka poput tvrtke Huawei, baš kao što su druge velike sile često iskorištavale položaj svojih tvrtki ili mogućnosti u telekomunikacijama.

Iz te šire povijesne perspektive, dokazi mogu navesti mnoge promatrače da zaključe da je opreznost oko uloge tvrtke Huawei u telekomunikacijskim mrežama opravdana, čak i ako su motivi tvrtke doista isključivo komercijalni, njezina obećanja o „bez sigurnosnih rupa i špijuniranja“ vjerodostojna i Peking iskren u svojoj posvećenosti poštivanju tih obećanja.

Šire gledano, kako pokazuje ovo izvješće, mnoge značajke telekomunikacijskog natjecanja velikih sila koje se danas smatraju novima vuku korijene iz prošlosti. Tijekom povijesti ponavljalo se nekoliko tema:

- *Moć:* Kontrola nad telekomunikacijskim mrežama oblik je političke moći od svog osnutka prije više od 150 godina. Velika Britanija iskoristila je svoju ulogu u telekomunikacijama i radiju, Sjedinjene Države to su vjerojatno učinile u moderno doba interneta, a postoji razlog za zabrinutost da bi Kina to mogla pokušati učiniti danas.

- *Nezainteresiranost*: Duga razdoblja mira i prosperiteta dovela su do nezainteresiranosti telekomunikacijskim rizicima. U 19. stoljeću velike su se sile zadovoljile oslanjanjem na strane tvrtke i mreže kojima one upravljaju, baš kao što su danas države bile spremne prihvatiti kinesku telekomunikacijsku opremu i rad. No, na kraju se oslanjanje na potencijalne konkurente ili protivnike pokazalo pogubnim za zemlje poput Njemačke i preoblikovalo svjetsku politiku.

- *Iskorištavanje:* Nova telekomunikacijska tehnologija uvijek je dovodila do novih pokušaja da je se presretne, napadne ili iskoristi. Unatoč nadama da šifriranje može zakomplicirati kineske pokušaje da presretnu moderne komunikacije, prošla razdoblja velikih nada u šifriranje srušila su se korisničkom pogreškom i odlučnim pokušajima suparničkih država da ih razbiju, kao što je Njemačka otkrila kad je Velika Britanija razbila njezine navodno „neprobojne“ šifre. Poniznost bi trebala pratiti svaki val navodno sigurnih tehnologija.

- *Prvaci:* Države često traže vlastite prvake u telekomunikacijama, posebno kad rastu napetosti velikih sila. Kineska je vlada ponosna na postignuća tvrtke Huawei i zalaže se za nju diljem svijeta, čak i prijeteći državama koje odbijaju njezinu tehnologiju. Bilo bi neobično da tvrtka koja je tako blizu matične vlade bude imuna na državni pritisak kad toliko drugih telekomunikacijskih prvaka u povijesti nije bilo.

- *Standardi*: Telekomunikacijski standardi mogu odrediti tko ima mrežnu moć, a Njemačka koristi organizaciju za normizaciju kako bi prekinula dominaciju Velike Britanije u bežičnom radiju. Danas je u tijeku to natjecanje u tijelima poput Međunarodne telekomunikacijske unije, a uloga tvrtke Huawei u njoj sugerira potrebu razmatranja hoće li njezini standardi omogućiti Kini da preoblikuje telekomunikacije.

- *Napad:* Sigurnost mreže ne predstavljaju samo presretanje i sigurnost podataka, već i napad na cijelu mrežu ili pristup vanjskim mrežama. Velika Britanija odsjekla je Njemačku od svjetskih telegrafskih mreža, a uloga tvrtke Huawei u mrežama mogla bi je osnažiti da isključi mreže u zemljama u kojima upravlja opremom, čak i ako ne može lako pristupiti podacima.

- *Odlučnost:* Mnoge države odbacuju stupanj u kojem protivnik može učiniti izvanredne pokušaje da kompromitira njihove mreže, a kad se to dogodi suočene su s neugodnim iznenađenjem. Sposobnost Velike Britanije da razotkrije njemačke šifre u Drugom svjetskom ratu pokušajima industrijskih razmjera i američka sposobnost prisluškivanja

unutarnjih sovjetskih podmorskih kabela koje je navodno nemoguće prisluškivati pokazuje dubinu do koje će velike sile ići da pristupe obavještajnim podacima o kritičnim signalima. I Kina će vjerojatno poduzeti takve maksimalne pokušaje, pa čak i ako će tvrtki Huawei biti teško učvrstiti svoj položaj u modernim mrežama, podcjenjivanje snalažljivosti i pokreta odlučnog konkurenta poput Kine motiv je koji se ponavlja u telekomunikacijskom natjecanju.

Kao što ovo izvješće pokazuje, mnoge značajke igre velikih sila u telekomunikacijama ostaju iste, iako se igrači mogu razlikovati.

O autorima

Rush Doshi bio je direktor Inicijative kineske strategije tvrtke Brookings i suradnik u vanjskoj politici tvrtke Brookings. Također je bio suradnik u kineskom centru Paul Tsai China u sklopu pravnog fakulteta Yale i bio je dio početne klase stipendista Wilson China. Njegovo istraživanje usredotočeno je na veliku kinesku strategiju, kao i na pitanja indo-pacifičke sigurnosti. Doshi je autor knjige *The Long Game: China's Grand Strategy to Displace American Order (Duga igra: velika strategija Kine za svrgavanje američkog uređenja)*, koju izdaje Oxford University Press. Trenutno služi u Bidenovoj dministraciji.

Kevin McGuiness nedavno je surađivao s organizacijom Brookings kao stručnjak iz odjela Skillbridge u sklopu Ministarstva obrane, gdje je sudjelovao u raznim projektima u okviru Centra za istočnoazijske političke studije. Veteran je ratnog zrakoplovstva i nedavno je završio službenu dužnost kao dio osoblja na zrakoplovnoj akademiji Sjedinjenih Država, vodeći tečajeve iz međunarodnih odnosa i azijske politike. Također je nedavno radio kao istraživač u Centru za proučavanje kineskih vojnih poslova Instituta za nacionalne strateške studije, gdje se usredotočio na modernizaciju PLA i sigurnost u Indo-pacifičkoj aziji.

Priznanja

Autori se žele zahvaliti bivšim pripravnicima Isabelli Lu, Zijin Zhou i Gaoqi Zhangu na njihovoj istraživačkoj pomoći u ovom projektu, nekoliko anonimnih recenzenata, Claire Harrison i Tedu Reinertu na uređivanju izvješća te Chrisu Krupinskom i Rachel Slattery na izgledu i web-dizajnu. Organizacija Brookings zahvalna je Državnom tajništvu SAD-a i Institutu za izvještavanje o ratu i miru na financiranju ovog istraživanja.

Ovo je izvješće dovršeno prije službe Rusha Doshija u vladi, uključuje samo otvorene izvore i ne odražava nužno službenu politiku ili stav bilo koje organizacije američke vlade.

Brookings Institution neprofitna je organizacija posvećena neovisnim istraživanjima i političkim rješenjima. Njezina je misija provoditi visokokvalitetna, neovisna istraživanja i, na temelju tih istraživanja, pružati inovativne, praktične preporuke za kreatore politike i javnost. Zaključci i preporuke bilo koje publikacije organizacije Brookings isključivo su zaključci njezinih autora i ne odražavaju stavove organizacije, uprave ili drugih znanstvenika.

[1] Steven Chase, Robert Fife i Barrie McKenna, "Trudeau Refuses to Let 'politics Slip into' Decision on Huawei," The Globe and Mail, 15. listopada 2018., https://www.theglobeandmail.com/politics/article-trudeau-refuses-to-let-politics-slip-into-decision-on-huawei/; Greg Quinn i Josh Wingrove, "Trudeau Says Politics Won't Factor Into Huawei 5G Decision," Time, 19. prosinca 2018., https://time.com/5485141/justin-trudeau-huawei-5g-decision-politics/.

[2] Daniel R. Headrick, The Invisible Weapon: Telecommunications and International Politics, 1851-1945 (Oxford, U.K.: Oxford University Press, 1991.), poglavlje 1.

[3] Ibid., napomena Daniela R. Headricka.

[4] Ibid.

[5] Ibid.

[6] Ibid., napomena Daniela R. Headricka.

[7] Heidi Tworek, News from Germany: The Competition to Control World Communications, 1900-1945 (New York: Harvard Historical Studies, 2019.).
[8] Daniel R. Headrick, The Invisible Weapon.
[9] „NH 79949 Cienfuegos Cable-Cutting Operation, 11 May 1898," Naval Historical Center Online Library, https://www.history.navy.mil/content/history/nhhc/our-collections/photography/us-people/b/baker-benjamin-f/nh-79949.html.
[10] Ibid., poglavlje 5.
[11] Jonathan Winkler, "Information Warfare in World War I," The Journal of Military History 73, br. 3 (2009.): 845–67, https://doi.org/10.1353/jmh.0.0324.
[12] Cameron McR. Winslow, "Cable-Cutting at Cienfuegos," 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," War on the Rocks, 6. studenoga, 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," *Army History* 46 (1998.): 14–21, https://www.jstor.org/stable/26304991.
[14] Jonathan Winkler, „Silencing the Enemy.
[15] „Spanish American War: Telegraphy and Cable Cutting, Introductory Essay," 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.
[17] Library of Congress, George Grantham Bain Collection, https://www.loc.gov/pictures/item/2014683102/.
[18] Iako Heidi Tworek primjećuje, njena vlastita uloga često je bila napuhana u razvoju ove tehnologije. Heidi Tworek, *News from Germany*.
[19] Marc Raboy, "The First Company That Wanted to 'Connect the World' Wasn't Google or Facebook," Media@LSE, 24. kolovoza, 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, 12–13.
[21] Michael Friedewald, "Telefunken vs. Marconi, or the Race for Wireless Telegraphy at Sea, 1896-1914," SSRN (9. siječnja, 2014.): https://doi.org/10.2139/ssrn.2375755.
[22] Ibid.
[23] Marc Raboy, Marconi: The Man Who Networked the World (Oxford, U.K.: Oxford University Press, 2016.), 226–28.
[24] Na primjer, tvrtka Telefunken bila je aktivna čak i u područjima u kojima Njemačka nije imala veliku kolonijalnu prisutnost, poput Latinske Amerike.
[25] George Johnson, ed., *The All Red Line: The Annals and Aims of the Pacific Cable Project* (Ottawa: James Hope and Sons, 1903.), 10, at Internet Archive, https://archive.org/details/allredlineannals00johnuoft/page/n11/mode/2up.
[26] Gordon Corera, "How Britain Pioneered Cable-Cutting in World War One," BBC News, 15. Prosinca, 2017., https://www.bbc.com/news/world-europe-42367551.
[27] Jonathan Winkler, "Information Warfare in World War I," 847.
[28] P. M. Kennedy, "Imperial Cable Communications and Strategy, 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," 849.
[30] Ibid., 851.
[31] Gordon Corera, "Why Was the Zimmermann Telegram so Important?," BBC News, 17. siječnja, 2017., https://www.bbc.com/news/uk-38581861; Patrick Beesly, Room 40: British Naval Intelligence 1914-18 (San Diego: Harcourt Brace Jovanovich, 1982.).
[32] C. O. Nordensvan and Valdemar Langlet, *Det stora världskriget* [The Great World War] (1915.), at Wikimedia Commons, https://commons.wikimedia.org/wiki/File:German_WW_I_field_telegraph_002.jpg.
[33] Jonathan Winkler, "Information Warfare in World War I."
[34] Wilhelm Flicke, "The Beginnings of Radio Intercept in World War I: A Brief History by a German Intelligence Officer," 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 (Newton Abbot, U.K.: David & Charles Ltd, 1973.); Prit Buttar, Collision of Empires: The War on the Eastern Front in 1914 (Oxford, U.K.: Osprey Publishing, 2014.).

[36] Matt Crypto, „The rotors of a Lorenz SZ42 cipher machine on display at Bletchley Park museum," at Wikimedia Commons, https://commons.wikimedia.org/wiki/File:SZ42-6-wheels.jpg.
[37] George I. Beck, „Military Communication - The Advent of Electrical Signaling," Britannica, https://www.britannica.com/technology/military-communication.
[38] Harry Hinsley, „The Influence of ULTRA in the Second World War" (lecture, Cambridge, U.K., October 19, 1993), http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF.
[39] $1x10^{170}$ moguće postavke.
[40] „Bletchley Park Remembers Polish Code Breakers," BBC News, 14. srpnja, 2011., https://www.bbc.com/news/uk-england-beds-bucks-herts-14141406.
[41] Gordon Welchman, The Hut Six Story: Breaking the Enigma Codes (Cleobury Mortimer, U.K.: Classic Crypto Books, 1997.).
[42] Harry Hinsley, „The Influence of ULTRA."
[43] Ibid.
[44] Za primjer pogledajte Jerry Roberts, Lorenz: Breaking Hitler's Top Secret Code at Bletchley Park (Cheltenham, U.K.: History Press, 2017.).
[45] F. W. Winterbotham, The Ultra Secret (New York: Harper & Row, 1974.), 154., 191.
[46] Harry Hinsley, "The Influence of ULTRA."
[47] Calder Walton, "The Spies Who Came In From the Continent," Foreign Policy, 27. travnja, 2019., https://foreignpolicy.com/2019/04/27/the-spies-who-came-in-from-the-continent-espionage-britain-brexit/.
[48] U.S. Navy, at Wikimedia Commons, https://commons.wikimedia.org/wiki/File:USS_Halibut_with_bow_thruster.jpg.
[49] Anna Borshchevskaya, „The Soviets' Unbreakable Code," Foreign Policy, 27. travnja, 2019., https://foreignpolicy.com/2019/04/27/the-soviets-unbreakable-code-fialka-encryption-espionage-russia-kgb-spy/.
[50] Daniel R. Headrick, The Invisible Weapon, poglavlje 4.
[51] Sherry Sontag, Christopher Drew, and Annette Lawrence Drew, Blind Man's Bluff: The Untold Story of American Submarine Espionage (New York: Public Affairs, 1998.), 222.
[52] Ibid.
[53] Ibid., 223.
[54] Ibid.
[55] Matt Blitz, "Navy Divers and Their Daredevil Mission to Spy on the Soviet Union at the Bottom of the Sea," Popular Mechanics, 30. ožujka, 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 (Washington, DC: Georgetown University Press, 2013.), 109–14; Matt Blitz, "Navy Divers."
[57] Damien McGuinness, „How a Cyber Attack Transformed Estonia," BBC News,27. travnja, 2017., https://www.bbc.com/news/39655415; Rain Ottis, „Analysis of the 2007 Cyber Attacks Against Estonia From the Information Warfare Perspective," (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," Small Wars Journal, 6. siječnja, 2011., https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008; Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, „Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war," Security Dialogue 43, br. 1 (2012.): 3–24, https://journals.sagepub.com/doi/10.1177/0967010611431079.
[59] Pavel Polityuk and Jim Finkle, „Ukraine Says Communications Hit, MPs Phones Blocked," Reuters, 4. ožujka, 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," Jamestown Foundation, 24. svibnja, 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," Wired, 20. lipnja, 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," U.S. Department of Justice, 19. listopada, 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," (congressional testimony, 28. lipnja, 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," *The Hill,* 5. siječnja, 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," Council on Foreign Relations, https://www.cfr.org/cyber-operations/titan-rain.
[64] Garrett Graff, „China's Hacking Spree Will Have a Decades-Long Fallout," Wired, 11. veljače, 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," *The Wall Street Journal,* 8. rujna, 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," The Wall Street Journal, 12. veljače, 2020., https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.
[67] Joe Parkinson, Nicholas Bariyo, and Josh Chin, „Huawei Technicians Helped African Governments Spy on Political Opponents," The Wall Street Journal, 15. kolovoza, 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," Bloomberg, 25. lipnja, 2020., https://www.bloomberg.com/news/articles/2020-06-25/hidden-back-door-embedded-in-chinese-tax-software-firm-says.