Pertemuan Huawei dengan sejarah: Kekuatan besar dan risiko telekomunikasi, 1840-2021

Rush Doshi dan Kevin McGuiness

Brookings Institution, Maret 2021

Ringkasan Eksekutif

Pada akhir tahun 2018, di tengah kekhawatiran Amerika terkait apakah Kanada akan mengizinkan akses Huawei ke jaringan telekomunikasinya, Perdana Menteri Kanada Justin Trudeau menyampaikan serangkaian pernyataan yang sejalan dengan kebijaksanaan konvensional hampir seluruh dunia. "Ini tidak seharusnya menjadi keputusan politik," ia menegaskan pada saat itu, dan Kanada tidak akan "membiarkan keterlibatan politik dalam pengambilan keputusan" terkait peran Huawei dalam jaringannya.[1]

Gagasan bahwa politik kekuasaan dapat dihilangkan dari persoalan telekomunikasi bukan hanya gagasan yang optimistis, tetapi juga tidak sejalan dengan sejarah telekomunikasi. Laporan ini menelusuri sejarah tersebut, dan menunjukkan bagaimana kekuatan dan telekomunikasi hampir selalu erat kaitannya. Ketika negara mengabaikan keterkaitan tersebut dan kurang memedulikan keamanan jaringan mereka sendiri, hasilnya tidak menguntungkan dan bahkan terkadang membahayakan.

Laporan ini mengkaji beberapa kasus penting terkait persaingan kekuatan besar di bidang telekomunikasi yang dimulai sejak awal terciptanya sistem telekomunikasi listrik pada tahun 1840-an. Kasus-kasus ini menunjukkan bahwa banyak persoalan yang dihadapi oleh para pembuat kebijakan saat ini memiliki kemiripan dengan yang terjadi dahulu. Meski persoalan keamanan jaringan dan infrastruktur 5G saat ini mungkin terasa baru, hal ini justru mengingatkan pada perselisihan yang terlupakan sejak awal terciptanya sistem telekomunikasi listrik sekitar 150 tahun yang lalu. Selain itu, banyak elemen umum dari persaingan telekomunikasi saat ini — seperti penggunaan badan penetapan standar, subsidi negara, perantara, perang informasi, pasar negara berkembang, dan enkripsi untuk memperoleh keuntungan — dikembangkan lebih dari satu abad yang lalu, dengan pelajaran penting untuk persoalan saat ini.

Berikut adalah beberapa pelajaran penting yang dapat diambil:

1. **Kendali atas jaringan telekomunikasi global merupakan bentuk kekuatan politik.** Jaringan 5G diharapkan dapat membentuk fondasi ekonomi yang lebih cerdas dan terhubung ke banyak perangkat dan sensor. Tiongkok, yang ingin membangun jaringan ini di seluruh dunia, telah memberikan subsidi kepada berbagai perusahaan dan proyek 5G terdepan di seluruh dunia sebagai bagian dari inisiatif "Digital Silk Road". Usaha tersebut sejalan dengan upaya Inggris dalam mencapai dominasi jaringan ketika sistem telegraf diciptakan. Inggris memperoleh keuntungan selama lebih dari enam dekade dengan terus meningkatkan ketergantungan negara lain pada jaringannya — bahkan dengan membebaskan biaya dan melepaskan keuntungan ekonomi untuk menarik minat negara lain pada jaringannya —

selagi mengurangi ketergantungan Inggris pada jaringan asing. Inggris pada akhirnya mengendalikan lebih dari setengah lalu lintas kabel dunia, jaringan radio terbesar, dan armada kapal kabel terbesar. Dengan terciptanya "hegemoni informasi", Inggris dapat memutus Jerman dari hampir semua telekomunikasi global pada saat Perang Dunia I dan memaksa Berlin untuk mengalihkan lalu lintasnya melalui jalur milik Inggris yang rentan terhadap pengawasan Inggris, yang kemudian terbukti menentukan kekalahan Jerman dalam konflik tersebut.

2. **Periode perdamaian dan kesejahteraan yang panjang umumnya menimbulkan rasa puas diri terhadap risiko telekomunikasi.** Dalam 30 tahun terakhir, perdamaian pasca-Perang dingin dan globalisasi ekonomi bertepatan dengan kemajuan pesat dalam bidang telekomunikasi yang membuat banyak negara mengutamakan keuntungan komersial revolusioner daripada risiko politik dan keamanan, bahkan termasuk kepemilikan atau pengoperasian jaringan. Pembangunan serupa terjadi pada masa awal sistem telekomunikasi pada tahun 1840-an, yang juga bertepatan dengan masa yang relatif damai dan globalisasi yang berlanjut... yang berlanjut hingga Perang Dunia I. Selama masa itu, keinginan untuk meraih kesempatan komersial yang tampak menakjubkan dari teknologi komunikasi baru mengaburkan persoalan ketergantungan pada jaringan atau perusahaan asing. Inggris Raya memperoleh keuntungan dari kepuasan negara lain dengan meraih dan kemudian mengeksploitasi posisi utama dalam jaringan global, dengan kekuatan besar lainnya bergantung pada jaringannya.

3. **Ketika negara merasa puas dengan keamanan telekomunikasi mereka, hasilnya dapat membahayakan dan dapat mengubah politik dunia.** Selama puluhan tahun Jerman merasa puas dengan ketergantungannya pada jalur telekomunikasi Inggris dan pada saat Berlin menyadari risiko dari ketergantungan tersebut, sudah terlalu terlambat untuk mengubahnya. Ketika Perang Dunia I dimulai, Inggris telah memutus semua kabel milik Jerman dan memaksa Berlin untuk mengubah jalur lalu lintasnya melalui jaringan Inggris meski dengan risiko intersepsi, yang berujung dengan terbongkarnya "telegram Zimmerman", yang membantu membawa Amerika Serikat ke dalam perang. Demikian pula, kegagalan Rusia dalam transmisi radio nirkabelnya dalam Perang Dunia I memungkinkan Jerman untuk mencegat komunikasi, "melihat" pergerakan pasukan Rusia secara langsung, dan mengalahkan mereka dalam Pertempuran Tannenberg. Kemudian, dalam Perang Dunia II, kepercayaan diri Nazi yang berlebihan dalam menyandikan pesan mereka membuat mereka melakukan sedikit upaya untuk memperbarui sandi mereka, sehingga memungkinkan Inggris Raya memecahkan kode dan memperoleh kecerdasan yang diyakini mempersingkat lama perang dua hingga empat tahun. Dengan kekuatan informasi, bahkan kegagalan transmisi sinyal atau rasa puas diri negara lain dapat mengubah sejarah.

4. **Teknologi baru selalu menimbulkan upaya baru untuk mencegatnya.** Dengan diciptakannya kabel bawah laut juga menyebabkan upaya untuk memutus dan menyadap jalur tersebut sejak awal Perang Spanyol-Amerika; transmisi radio membangkitkan upaya pesaing untuk menangkap node jaringan dan untuk mencegat transmisi; dan dengan diciptakannya sandi yang canggih untuk melakukan enkripsi juga menyebabkan upaya pada skala industri untuk memecahkannya. Pada setiap zaman, beberapa pihak percaya bahwa

inovasi baru dalam bidang komunikasi mungkin lebih aman daripada inovasi sebelumnya. Namun, siklus inovasi dan eksploitasi terus berlanjut.

5. **Jaringan telekomunikasi tidak pernah netral secara politik, terutama pada saat ketegangan.** Pada tahun 2019, para eksekutif Huawei membuat janji "no-backdoor, no-spying" dan berjanji bahwa perusahaan mereka tidak akan terlibat dalam politik, dan pemerintah Tiongkok juga berkomitmen untuk menghormati janji tersebut. Namun, lebih dari satu abad yang lalu, perusahaan telekomunikasi dan pemerintah negara tempat perusahaan berasal membuat janji serupa di depan publik dan secara diam-diam melanggarnya dan bekerja sama pada masa damai dan masa perang. Misalnya, dominasi Inggris atas kabel bawah laut membuat Prancis, Jerman, dan Amerika mengusulkan untuk jalur tersebut tetap netral, bahkan pada masa perang. Perusahaan Inggris secara terbuka menyatakan sikap netralitas mereka tetapi pada kenyataannya tunduk pada kepentingan politik Inggris, terutama pada saat ketegangan besar, dan sepenuhnya melepaskan netralitas selama masa perang. Kekuatan yang berasal dari disrupsi atau intersepsi arus informasi pesaing biasanya terlalu memikat bahkan untuk ditolak oleh klaim netralitas yang tulus.

6. **Negara sering berupaya menciptakan sistem telekomunikasi mereka sendiri setelah menyadari kerentanan saat mengandalkan pesaing atau perusahaan lain.** Amerika Serikat saat ini kekurangan produsen utama stasiun pangkalan 5G, yang memicu perdebatan tentang apakah mereka harus berinvestasi di perusahaannya sendiri atau mengandalkan perusahaan sekutu. Hal ini juga memicu perselisihan tentang sejauh mana Huawei menjadi juara secara de facto. Perdebatan seperti ini juga pernah terjadi sebelumnya. Pada awal abad ke-20, banyak negara yang mengandalkan peralatan telekomunikasi atau jaringan negara lain lalu mulai membangun sistem mereka sendiri. Misalnya, Jerman mendorong dua perusahaan Jerman — Siemens & Halske dan AEG — untuk bersama-sama membangun teknologi milik Jerman sendiri yang menandingi dominasi Inggris dalam teknologi radio. Banyak negara terkemuka lainnya yang mendukung perusahaan yang, meski tampak tertutup, sebenarnya juga terlibat dengan berbagai negara yang mendukung mereka.

7. **Perjuangan untuk menetapkan standar telekomunikasi dapat menentukan negara mana yang akan memiliki kekuatan jaringan, dan biasanya mengharuskan negara untuk menjalin hubungan dengan sekutu dan mitra lainnya.** Negara yang teknologinya menjadi standar dominan dapat memiliki pengaruh yang lebih besar pada negara lain. Persaingan atas penetapan teknologi informasi saat ini memiliki kemiripan dengan kontes persaingan Anglo-Jerman atas jaringan radio. Inggris, melalui Marconi Company yang didukungnya, sangat mendominasi radio nirkabel sehingga semua kekuatan besar lainnya harus mengirimkan pesan melalui jaringan nirkabel Inggris, yang menolak untuk terlibat dengan stasiun nirkabel lainnya. Jerman pada akhirnya meraih kesuksesan dalam mematahkan dominasi penetapan standar Inggris yang melarang kebijakan "non-interkomunikasi" dengan bantuan kekuatan besar lainnya, termasuk Amerika Serikat dan Prancis — sebuah demonstrasi tentang bagaimana pendekatan koalisi yang serupa saat ini dapat digunakan oleh negara-negara liberal untuk menetapkan

atau menjaga standar teknologi informasi dan komunikasi (TIK) yang menguntungkan jika mereka bekerja bersama.

8. **Negara beralih ke enkripsi karena komunikasi mereka menjadi lebih mudah untuk dicegat, tetapi enkripsi sering kali memiliki batasan karena tekad musuh atau kesalahan pengguna.** Beberapa pihak berpendapat bahwa kekhawatiran akan peran Huawei dalam jaringan atau terkait kerentanan pada perangkat yang terhubung ke internet akan diatasi oleh enkripsi modern. Pendapat semacam ini memiliki sejarah yang panjang. Pada masa awal terciptanya sistem telekomunikasi seabad yang lalu, kemungkinan pesan telegraf dapat dibaca oleh orang lain yang mengendalikan node jaringan, atau radio tersebut dapat dicegat oleh peralatan dengar pasif, yang berujung dengan kemajuan enkripsi yang kadang menimbulkan rasa terlalu percaya diri. Mesin sandi rotor yang kompleks milik Jerman diyakini tidak dapat dipecahkan, tetapi kesalahan pengguna dan upaya pada skala industri dari Inggris memungkinkan Inggris Raya memecahkan kode-kode Jerman. Pembaruan berbiaya rendah untuk peralatan dan sandi Jerman bisa saja mengalahkan Inggris, tetapi keyakinan Berlin yang berlebihan dalam enkripsinya yang mencegahnya terjadi, menyebabkan kecerdasan yang dicegat tersebut mengubah jalannya perang. Enkripsi menyeluruh jauh lebih canggih daripada upaya enkripsi sebelumnya, tetapi sejarah menunjukkan bahwa kerendahan hati juga diperlukan.

9. **Banyak negara mengabaikan sejauh mana musuh dapat melakukan upaya luar biasa untuk membahayakan jaringan mereka.** Di tengah perdebatan tentang telekomunikasi modern, perlu diperhatikan bahwa negara yang memprioritaskan kemudahan atau perdagangan, dan memilih mengambil jalan pintas keamanan, sering kali dikejutkan dengan upaya yang dilakukan musuh yang bertekad untuk membahayakan jaringan mereka. Dalam Perang Dunia I, Jerman terkejut dengan kecepatan dan kekejaman Inggris yang memotong semua kabel yang digunakan Jerman untuk mengakses dunia luar; Demikian pula, para komandan Rusia terkejut ketika kesalahan radio mereka menyebabkan kekalahan mereka di Tannenberg. Dalam Perang Dunia II, Jerman tidak mengharapkan Inggris membangun operasi pemecahan kode berskala industri yang sangat terpusat dan mampu mengeksploitasi kesalahan komunikasi Jerman — tak peduli betapa sepele atau kecilnya — untuk memecahkan kode Jerman. Selain itu, selama Perang dingin, Soviet tidak pernah mengenkripsi saluran telepon bawah air internal yang mereka yakini berada di luar jangkauan Amerika Serikat, tetapi Washington masih menemukan cara untuk menyadapnya dan memperoleh sumber kecerdasan yang berharga.

10. **Keamanan jaringan tidak hanya tentang intersepsi, tetapi juga tentang penolakan.** Beberapa perdebatan tentang peran Huawei dalam jaringan menekankan pada persoalan keamanan data, tetapi dapat memperoleh manfaat dari pertimbangan penolakan jaringan yang lebih besar, yang merupakan bagian penting dari persaingan kekuatan besar atas telekomunikasi. Masa awal terciptanya sistem telegraf menyaksikan para kekuatan besar yang berupaya untuk memotong kabel dan menolak komunikasi, dan mencapai puncaknya dalam operasi Inggris yang belum pernah dilakukan sebelumnya dan direncanakan dengan baik untuk memutuskan semua kabel di seluruh dunia yang dapat menghubungkan Jerman

ke dunia luar. Terkadang, suatu negara dapat membahayakan keamanannya dalam mengatur strategi penolakan jaringan, tetapi akan tetap melanjutkannya jika yakin akan lebih membahayakan lawannya.

Kekuatan besar dan telekomunikasi

"Kerajaan-kerajaan besar berusaha keras untuk mempercepat arus informasi," seperti yang tercatat dalam salah satu sejarah telekomunikasi. "Bangsa Romawi membangun jalan, Bangsa Persia dan Mongol telah menciptakan pacuan kuda, Inggris mensubsidi kapal uap."[2] Namun, meski banyak negara menginginkan informasi, arus informasi tetap terbatas hingga terciptanya sistem telegraf modern. Elektrifikasi arus informasi menciptakan sistem telekomunikasi modern, dan dengannya, pola-pola persaingan kekuatan besa terkait.

Beberapa dekade awal telekomunikasi modern tersebut, yang berlangsung dari tahun 1840 hingga Perang Dunia I, memiliki karakteristik penting yang mirip dengan saat ini. Periode tersebut, seperti era pasca Perang dingin saat ini, merupakan salah satu perdamaian kekuatan besar yang membuat negara-negara terdepan "kurang peka" terhadap persoalan politik dan keamanan dalam jaringan telekomunikasi.[3] Ketika kekuatan besar membangun jaringan nasional dan internasional pada abad ke-19, banyak di antaranya yang awalnya tidak keberatan untuk membiarkan industri memegang kendali, mengabaikan nasionalitas perusahaan swasta, dan meremehkan risiko kendali jaringan telekomunikasi oleh musuh. Manfaat dari perubahan revolusioner dalam telekomunikasi — yang sering kali disebut "penghancuran ruang dan waktu"[4] — dahulu terlihat begitu jelas dan menggiurkan sehingga "kepemilikan atas kabel dianggap sebagai masalah kecil."[5] Telegraf pada masa itu lebih terkait dengan bisnis daripada politik, mencatat seorang sejarawan dalam pengamatannya yang mungkin dapat dengan mudah diterapkan pada sebagian kegembiraan awal dari teknologi informasi modern dan yang paling baru: 5G.[6]

Periode ini tidak berlangsung lama. Negara seperti Peru pada tahun 1879 dan kemudian Amerika Serikat pada tahun 1898 merupakan negara pertama yang memutus jaringan telekomunikasi lawan. Seiring dengan meningkatnya ketegangan kekuasaan, negara-negara di seluruh dunia menyadari bahwa beberapa negara — seperti Inggris Raya — berhasil mempertahankan perdamaian ini dengan baik, dan melalui perusahaan swasta, mereka memegang kendali atas komunikasi internasional.

Karena makin takut akan ketergantungan pada jaringan kabel bawah laut Inggris, negara-negara seperti Prancis dan Jerman memberikan subsidi besar terhadap pengembangan jaringan mereka sendiri seperti halnya dalam pengembangan yang tidak terlalu berbeda dengan Tiongkok yang memberikan subsidi dan perlindungan terhadap perusahaan yang mengembangkan teknologi informasinya seperti Alibaba, Baidu, Tencent, Tencent, dan Huawei. Begitu pula menurut sejarawan Heidi Tworek, negara yang bersaing dengan Inggris juga mengandalkan generasi teknologi telekomunikasi masa depan — "telegraf nirkabel", yang lebih dikenal sebagai radio — berharap untuk mengurangi ketergantungan pada kabel telegraf bawah laut milik Inggris.[7] Sementara Inggris memimpin dalam hal ini, Jerman menolak mengandalkan jaringan Inggris. Jerman membangun jaringannya sendiri bersama berbagai perusahan dari bagian dunia lain yang kurang terhubung — Amerika Latin, Afrika, Asia — seperti halnya dengan perluasan perusahaan

teknologi Tiongkok ke berbagai negara berkembang dan tekad Beijing untuk menetapkan standar jaringan 5G.

Sepanjang periode ini, banyak elemen dari persaingan kekuatan atas telekomunikasi yang kadang terabaikan pada saat ini sering kali dianggap cukup serius oleh berbagai negara pada era itu. Jerman, yang frustrasi dengan dominasi Inggris atas jaringan radio, menggunakan badan penetapan standar untuk mematahkan dominasi Inggris — sebuah taktik yang menunjukkan bahwa badan-badan tersebut tidak kalah pentingnya pada era itu daripada sekarang. Selain itu, ketika sistem telekomunikasi berubah menjadi nirkabel dan lebih mudah untuk dicegat, kekuatan besar pun menempatkan keyakinan mereka pada enkripsi — terkadang mengabaikan pengoperasian jaringan yang disiplin dengan berasumsi bahwa "penyandian" — langkah-langkah terperinci untuk mengenkripsi atau mendekripsi pesan — akan menyelesaikan masalah tersebut, keyakinan yang hampir selalu terbukti salah karena kesalahan pengguna. Pandangan ini mempunyai kesamaan dengan asumsi modern terkait ketidakamanan jaringan telekomunikasi, dan keyakinan yang dikemukakan oleh beberapa pihak terkait Huawei bahwa enkripsi akan lebih menetralkan risiko dari akses Tiongkok ke jaringan telekomunikasi negara lain.

Ketika perdamaian kekuatan besar berakhir dan perang meletus, kepentingan politik terkait bidang telekomunikasi — yang tidak selalu jelas pada masa damai — tiba-tiba tampak jelas. Keberhasilan Jerman dalam mencegat transmisi Rusia dalam Perang Dunia I berujung pada kemenangan yang begitu menyeluruh dalam Pertempuran Tannenberg yang mengubah jalannya perang dan membantu mempercepat keluarnya Rusia dari konflik tersebut. Dominasi Inggris atas kabel bawah laut dalam Perang Dunia I juga begitu menyeluruh hingga dapat memutus Jerman dari sistem telekomunikasi global, mengubah lalu lintas kabel Jerman melalui jaringan Inggris, dan akhirnya mengungkap telegram Zimmerman, yang membantu membawa Amerika Serikat ke dalam konflik. Dalam Perang Dunia II, Inggris meraih keberhasilan intelejen lagi dengan memecahkan enkripsi Jerman yang dianggap tidak dapat dipecahkan, yang berakhir dengan keberhasilan Inggris dalam mendapatkan intelijen yang sangat berharga dan menurut sejarah resmi Inggris, mempersingkat perang di Eropa hingga beberapa-tahun. Kasus-kasus ini menunjukkan bahwa keamanan telekomunikasi bukan hanya masalah taktik medan perang, tetapi juga masalah persaingan politik yang dapat menentukan nasib kekuatan besar dan membentuk sejarah dunia.

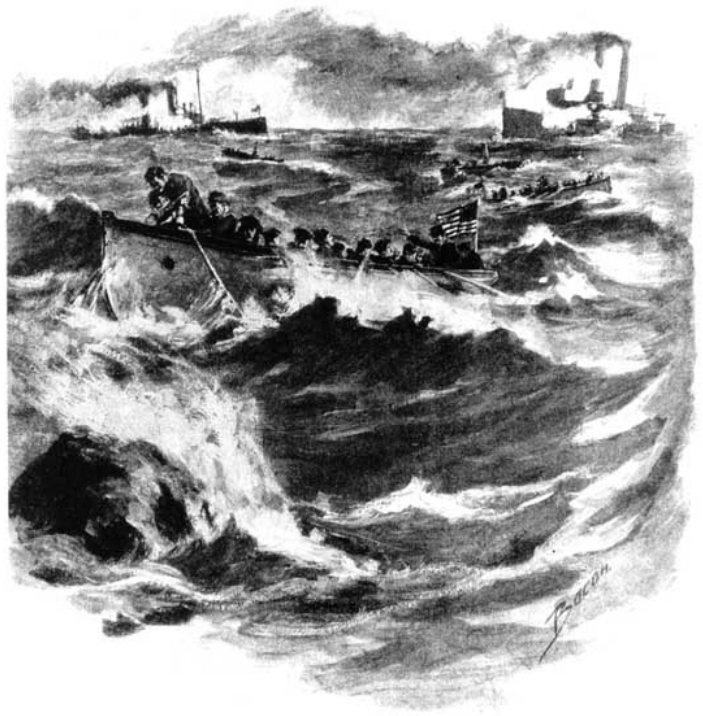
Ketika dunia berganti ke Perang Dingin AS-Soviet, keunggulan Inggris tergerus oleh kekuatan Amerika dengan perkembangan teknologi yang membuat jaringan sebelumnya kurang relevan. Hal ini menunjukkan bahwa penting bagi kekuatan besar untuk tetap menjadi yang terdepan dalam bidang teknologi. Pada era baru tersebut, persaingan telekomunikasi terus berlanjut di sepanjang jalur yang sama. Misalnya, Amerika Serikat memelopori cara baru untuk menyadap kabel bawah laut yang terkubur begitu dalam dan dianggap sangat aman sehingga pesan-pesan di dalamnya sering kali dibiarkan tanpa enkripsi. Persaingan juga berganti ke domain lain — seperti satelit dan infrastruktur internet — meski sebagian besar dari sejarah ini masih berjalan dan, dalam sebagian besar kasus, tetap rahasia.

Telekomunikasi, seperti yang tampak dalam rangkaian kasus ini, selalu bersifat politik. Eksploitasi terhadap teknologi dan kemampuan ini secara umum meningkat seiring dengan perkembangannya. Segera setelah metode komunikasi baru tiba, kekuatan besar biasanya mencari cara untuk mencegat atau menginterupsinya. "Komunikasi elektronik sering kali digambarkan sebagai salah satu pencapaian besar umat manusia," kata seorang ahli sejarah telekomunikasi, "tetapi ketika kita melihatnya dari sudut pandang keamanan, kita melihat gambaran yang sama sekali berbeda, karena

keamanan bukanlah masalah teknis tetapi masalah sosial dan politik." Selain itu, "selama politik belum membaik," katanya, "telekomunikasi memiliki sisi yang gelap."[8]

Sekarang, kita beralih ke ringkasan tema utama selama hampir dua abad persaingan telekomunikasi.

1. Perang Spanyol-Amerika: Batasan netralitas kabel



Gambaran ekspedisi pemotongan kabel AS di Cienfuegos, diterbitkan tahun 1907. Operasi tersebut menunjukkan bahwa kabel telegraf bawah laut tidak akan diperlakukan secara netral selama konflik bersenjata, bahkan oleh kekuatan besar yang pernah mengusulkan netralitas kabel.

Sumber: Naval Historical Center Online Library[9]

Ketika kabel-kabel bawah laut mulai tersebar ke seluruh dunia pada abad ke-19, beberapa pemimpin kekuatan — termasuk Prancis, Jerman, dan Amerika Serikat — mengusulkan agar kabel-kabel tersebut dipisahkan dari politik internasional. Pada tahun 1858, ketika salah satu kabel trans-Atlantik pertama dikirimkan, Presiden AS James Buchanan mendesak Ratu Victoria untuk memastikan bahwa jalur telegraf baru tersebut tetap "netral untuk selamanya… bahkan saat masa perang."[10]

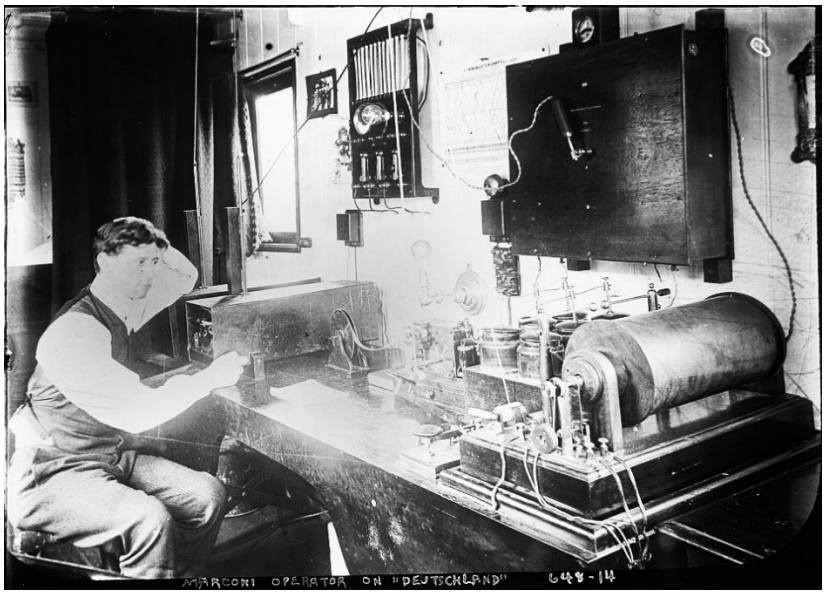
Namun, begitu perang meletus, prinsip netralitas yang dijunjung tinggi pun dilupakan. Dua dekade setelah pesan Buchanan, Peru memotong jalur kabel Chili yang menimbulkan perselisihan antara keduanya.[11] Perselisihan tersebut hanya mendapat sedikit perhatian, tetapi saat Amerika Serikat — yang sebelumnya menjunjung tinggi netralitas kabel — memotong kabel di Atlantik dan Pasifik pada saat Perang Spanyol-Amerika, dunia menyatakan perhatiannya.

Pemotongan kabel oleh Amerika telah direncanakan sebelum konflik terjadi. Di wilayah Atlantik, AS berharap dapat memisahkan Spanyol dari pasukannya di Kuba. “Pengasingan Havana, tentu saja, sangat penting,” menurut salah satu majalah Amerika, yang pada saat itu menuntut Amerika Serikat untuk “menutup Havana dari semua komunikasi telegraf dengan dunia luar.”[12] Amerika Serikat memulai dengan memotong lalu lintas Spanyol yang melintasi wilayah Amerika di Florida. Kemudian, Amerika mengirimkan pasukan kecil untuk menghancurkan node telekomunikasi utama di Cienfuegos, yang memutus kota Havana dan sebagian besar wilayah Kuba barat dari Spanyol. Setelah itu, Amerika Serikat menyerang berbagai kabel di wilayah Kuba timur serta kabel di wilayah Karibia yang menghubungkan Puerto Riko dengan Spanyol.[13] Bersama-sama, pemotongan kabel tersebut secara signifikan melemahkan kemampuan Spanyol untuk mengarahkan dan memimpin pasukan di Kuba.[14]

Di wilayah Pasifik, Amerika Serikat memotong satu-satunya kabel bawah laut antara Manila dan Hong Kong, yang secara efektif memutus Filipina dari Spanyol.[15] Keputusan tersebut juga merusak komunikasi AS, tetapi dianggap lebih merugikan Spanyol, dan Amerika Serikat dapat mengatasinya dengan mengirimkan satu kapal secara teratur ke Hong Kong untuk kembali mengirimkan pesan ke Washington.[16] Pasukan AS juga memotong kabel bawah laut di wilayah Filipina, yang makin melemahkan kemampuan Spanyol untuk mengendalikan pasukannya.

Perang Spanyol-Amerika mungkin merupakan konflik global pertama yang mencakup beberapa wilayah yang penting untuk telekomunikasi elektrik. Konflik ini juga menandai pertama kalinya satu kekuatan besar berupaya menolak akses lain ke kabel bawah laut. Sebelum konflik tersebut, telegraf masih cenderung dipandang sebagai ranah komersial, dan banyak pihak yang berharap kabel-kabel tersebut tetap dibatasi dari persaingan politik dan militer. Konflik tersebut membuktikan adanya batasan pada teknologi tersebut, dan menunjukkan bahwa kendali atas infrastruktur telekomunikasi serta kemampuan untuk menghilangkan keuntungannya bagi lawan geopolitik selalu menjadi kepentingan politik yang sangat penting.

2. Persaingan Inggris-Jerman: Membangun jaringan dan menetapkan standar



Operator radio Marconi Company dalam "Marconi Room" kapal laut Jerman SS Deutschland. Pengaruh Marconi Company sangat besar hingga karyawannya beroperasi di ruang radio Jerman meski Jerman mengkhawatirkan risiko penyadapan dan penolakan.

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

Penetapan standar teknologi, dan pengaruhnya pada sistem jaringan, adalah arena persaingan kekuatan besar yang telah lama ada dan tidak kentara. Negara yang teknologinya menjadi standar dominan dapat memiliki pengaruh yang lebih besar terhadap negara lain — suatu titik yang tidak hilang pada kekuatan yang makin meningkat, yang sering bekerja untuk mengurangi kerentanan mereka dengan menciptakan sistem paralel. Memang, persaingan Sino-Amerika atas ICT mengingatkan pada persaingan yang terjadi seabad lalu antara Jerman dan Inggris Raya untuk meraih dominasi infrastruktur ICT pada era itu, dengan kemiripan yang luar biasa dan pelajaran yang penting untuk saat ini.

Pada akhir abad ke-19, insinyur Italia Guglielmo Marconi, yang didukung oleh British Royal Navy, menciptakan telegraf nirkabel.[18] Penemuan ini merupakan suatu revolusi. Ketika dahulu kekuatan besar memotong kabel satu sama lain, dan ketika komunikasi kapal-ke-kapal dan kapal-ke-pantai sebelumnya sulit dilakukan, sistem Marconi memecahkan masalah tersebut dan tidak terlalu rentan terhadap interferensi.[19] Marconi pada akhirnya bekerja sama dengan Inggris Raya dan berhasil memonopoli transmisi radio. Ketika digabungkan dengan 60% saham Inggris dari jaringan kabel bawah laut dunia, Inggris mendominasi transmisi internasional. Keuntungan Inggris mengganggu Jerman, tetapi persaingan teknologi nirkabel juga "menghadirkan peluang bagi Jerman untuk mengendalikan infrastruktur internasional baru" dan "menghindari kabel Inggris", hingga pada akhirnya dominasi Inggris berakhir.[20]

Merasa rentan, Kaiser Wilhelm II memberi dukungan langsung kepada para ilmuwan dan insinyur Jerman saat mereka berhasil meniru desain Marconi, mematenkannya di Jerman, dan membangun jaringan radio mereka sendiri yang didanai oleh kontrak dengan militer Jerman.[21] Walaupun demikian, keunggulan radio jarak jauh Marconi membantu pendirian perusahaan yang didukung Inggris sebagai standar global, dan Marconi memanfaatkan pengaruh jaringan ini untuk mengusulkan kebijakan "non-interkomunikasi" dengan operator radio non-Marconi. Bisnis dan kapal laut Jerman tidak ingin terputus dari komunikasi global, sehingga mereka lebih memilih sistem yang didukung Inggris daripada Jerman.

Kaiser Wilhelm II makin memperkuat kebijakan industri Jerman untuk melawan standar Inggris. Dia dengan cepat memerintahkan dua perusahaan listrik Jerman, Siemens & Halske dan AEG, untuk bergabung bersama dan membangun teknologi alternatif milik Jerman sendiri, yaitu Telefunken. "Persaingan [domestik] di bidang telegraf nirkabel melemahkan daya saing Jerman," Kaiser menjelaskan, "dan memberi Marconi Company peluang untuk meraih monopoli di seluruh dunia" yang sebenarnya "bukan untuk kepentingan Jerman".[22] Di bawah perintah Kaiser Wilhelm II, Jerman mengejar proteksionisme dengan melarang sistem Marconi dalam beberapa kasus. Jerman mengejar pasar yang sedang berkembang dengan menjual teknologinya ke Amerika Selatan dan Afrika untuk menetapkan standar di wilayah tersebut dan mengamankan pendapatan.

Ketika upaya tersebut terbukti tidak memadai, Jerman meraih keberhasilan melalui badan-badan penetapan standar multilateral. Pada tahun 1906, Jerman mengorganisir kekuasaan besar bersama-sama dalam Konvensi Radiotelegraf Internasional pertama, yaitu konferensi yang membahas standar radio. Dalam konferensi tersebut, para anggotanya bersama-sama melarang kebijakan "non-interkomunikasi" Marconi, yang kemudian menghentikan monopoli Inggris dan membentuk duopoli Anglo-Jerman yang efektif.[23]

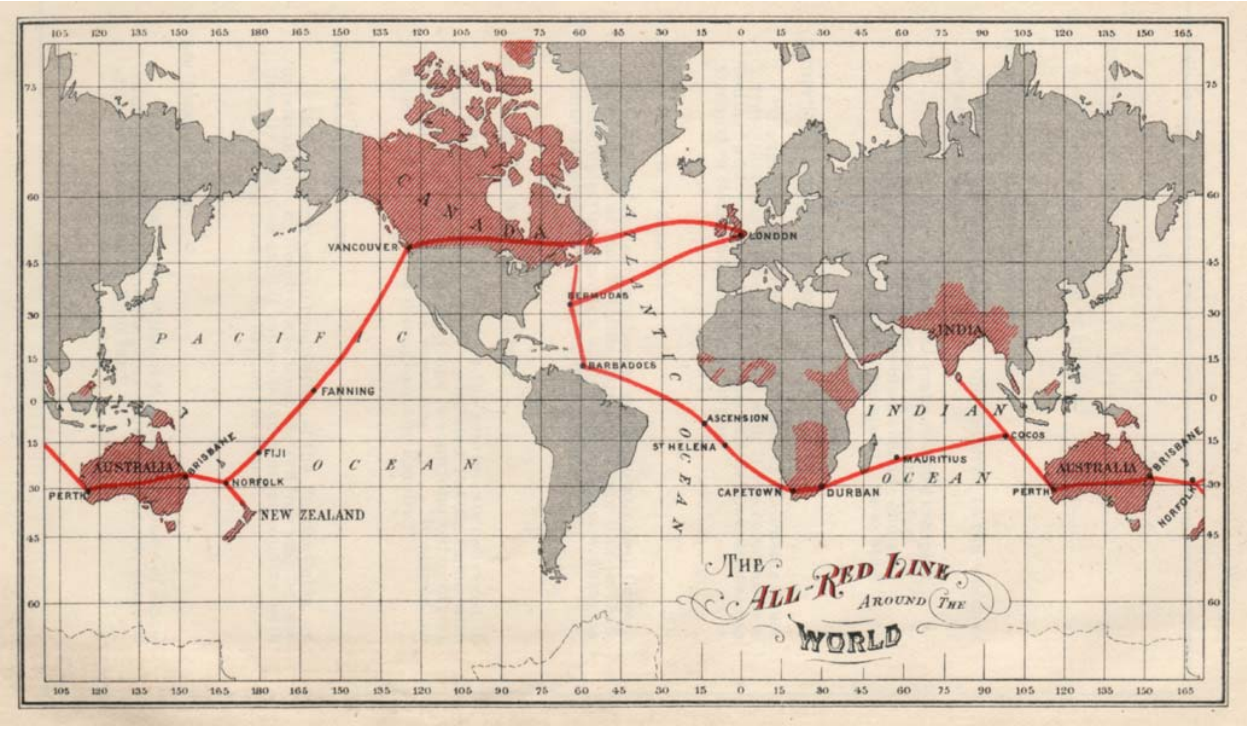
Persaingan Anglo-Jerman menunjukkan bahwa badan-badan penetapan standar tersebut mempunyai implikasi strategis yang besar. Tiongkok saat ini menggunakan banyak teknik yang digunakan oleh Jerman seabad yang lalu — kebijakan industri yang dipimpin negara, perlindungan negara, kontrak negara, integrasi sipil-militer, larangan terkait produk pesaing, penggabungan paksa, penargetan pasar negara berkembang, dan bahkan perjanjian internasional untuk menetapkan standar-standarnya — semuanya telah membantu berbagai perusahaan teknologi Tiongkok seperti Alibaba dan Tencent, pemilik WeChat dan AliPay, untuk menjadi juara lokal. Sejak saat itu, perusahaan-perusahaan ini telah berkembang di luar negeri dan sering kali tidak menargetkan pasar AS, tetapi — seperti Telefunken Jerman dahulu — pasar negara berkembang dengan keuntungan yang lebih rendah dan persaingan yang lebih sedikit.[24]

Tiongkok juga menyaingi standar dalam infrastruktur konektivitas internet. Pemerintah Tiongkok menginvestasikan miliaran agar pembuat chip Tiongkok dapat mengalahkan lawan dari Amerika dalam persaingan untuk menetapkan standar internet seluler 5G. Demikian pula, perusahaan-perusahaan Tiongkok seperti Huawei dan ZTE menerima pinjaman dari pemerintah untuk membangun infrastruktur konektivitas internet di berbagai negara berkembang. Seperti yang dicontohkan oleh Inggris, upaya-upaya ini tidak hanya menjadikan teknologi Tiongkok sebagai standar, tetapi juga menghadirkan peluang untuk pengawasan. Sementara itu, inisiatif Belt and Road meningkatkan kemungkinan bahwa standar "infrastruktur cerdas" di seluruh Asia,

khususnya sensor dan perangkat lunak terkait, mungkin ditentukan oleh Tiongkok dan Tiongkok mungkin menolak interoperabilitas perusahaan lainnya, sehingga menutup mereka dari industri kendaraan otonom dan industri lainnya.

Persaingan Anglo-Jerman dalam sistem telegraf menunjukkan bahwa Washington perlu menanggapi tantangan penetapan standar oleh Tiongkok dengan serius. Hal ini juga menawarkan jalan ke depan. Sama halnya dengan Jerman yang memanfaatkan konferensi internasional untuk menghentikan monopoli Inggris di bidang telegraf, Amerika Serikat dapat menetapkan atau mempertahankan standar ICT yang menguntungkan melalui perjanjian multilateral. Jika melakukannya, Amerika dapat mencegah Tiongkok membuat penetapan standar unilateral melalui perjanjian perdagangan bebas, pendukung negara, atau proyek infrastruktur.

3. Inggris dalam Perang Dunia I: Menerapkan hegemoni informasi



"All Red Line," jaringan kabel bawah laut Inggris yang mahal dibangun dengan redundansi yang sangat besar dan diatur sehingga tidak ada bagian yang melewati wilayah lawan. Investasi Jerman yang kurang memadai dalam jaringan telekomunikasi globalnya sendiri memungkinkan Inggris untuk memutus Jerman dari komunikasi global sementara Inggris secara umum tidak terpengaruh.

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

Upaya Jerman untuk menghentikan dominasi Inggris dalam bidang telekomunikasi pada awal abad ke-20 bukan karena alasan paranoia. Setelah Perang Dunia I pecah, Inggris berhasil memanfaatkan pengaruhnya yang besar dalam jaringan telekomunikasi untuk membentuk jalannya perang. Inggris memotong kabel-kabel Jerman, memantau transmisi Jerman, dan memaksa lalu lintas informasi Jerman ke jaringan yang dikendalikan Inggris — hingga mengungkap telegram Zimmerman, yang membantu membawa Amerika ke dalam perang.[26]

Inggris Raya bukanlah kekuatan besar pertama yang memotong atau memanipulasi jaringan telekomunikasi: Sebelumnya, Peru berhasil memutuskan hubungan Chili-Bolivia, Amerika Serikat telah memotong kabel Spanyol, dan Inggris telah memutuskan Boers dari pendukung mereka di Eropa dalam satu krisis dan manipulasi lalu lintas kabel ke Prancis dan negara lainnya.[27] Namun, berbagai upaya ini sangat dianggap serius dalam Perang Dunia I.

Inggris Raya adalah yang pertama kali memutuskan seluruh negeri dari jaringan telekomunikasi global umum, dilakukan pada hari pertama perang, sebuah rencana yang dibuat dengan hati-hati selama masa damai.[28] Dalam satu tahun, Inggris Raya menghancurkan kabel Jerman di seluruh

dunia: di Saluran Inggris, Laut Utara, Atlantik Utara, Amerika Selatan, sebagian besar Afrika, Timur Jauh, dan bahkan di beberapa negara netral yang menggunakan infrastruktur Jerman.[29]

Sebagai gantinya, Jerman mencoba memperluas jaringan radio yang dibangun Telefunken sepuluh tahun sebelumnya di Amerika Latin dan "Global South" sehingga dapat menjangkau seluruh dunia. Dalam upaya yang mirip dengan inisiatif Digital Silk Road Tiongkok, Berlin menawarkan pinjaman dan investasi bagi pemerintah yang tertarik dengan "keuntungan pengembangan radio" sehingga mereka bersedia menampung node komunikasi Jerman. Sebagai tanggapan, Inggris Raya meyakinkan sebagian besar negara-negara ini untuk menghentikan dukungan untuk menampung node radio Jerman atau secara aktif menyabotasenya.[30]

Tanpa jaringannya sendiri, Berlin tidak memiliki pilihan lain selain bergantung pada jaringan Inggris selama perang. Pada awalnya, Inggris secara diam-diam mulai memantau semua lalu lintas informasi yang melalui kabel mereka dan memanfaatkan keuntungan mereka untuk melancarkan perang informasi melawan Jerman, dengan secara selektif membocorkan lalu lintas informasi Jerman yang memalukan untuk merusak hubungannya dengan negara-negara netral. Ketika Jerman mengirimkan sebuah telegram yang menawarkan aliansi militer dengan Meksiko melawan Amerika Serikat — telegram Zimmerman yang terkenal — pesan tersebut melintasi jaringan Inggris dan dicegat serta didekripsi oleh Inggris Raya, yang kemudian membagikannya dengan pemerintah Amerika Serikat, yang kemudian membagikannya kepada publik Amerika Serikat.[31] Insiden tersebut membantu membawa Amerika Serikat ke dalam perang dan membentuk sejarah dunia serta pada akhirnya menjamin kekalahan Jerman.

Perang informasi Inggris melawan Jerman mengungkapkan bahaya yang ada ketika memberikan kekuatan kepada lawan untuk memantau lalu lintas informasi atau menghentikan akses telekomunikasi negara lain. Hal ini juga mengungkapkan bahwa jaringan yang diterima begitu saja oleh kekuatan-kekuatan besar pada masa damai sering kali ditolak pada masa perang, dan bahwa pengembangan node komunikasi pasti akan melibatkan pihak ketiga dan negara-negara netral.

4. Kemenangan Jerman di Tannenberg: Bahaya penyadapan

Stasiun telegraf lapangan nirkabel milik Jerman selama Perang Dunia I. Ketidakmampuan Rusia untuk mengenkripsi komunikasinya secara memadai di stasiun lapangannya menyebabkan kekalahan telak yang mengubah jalannya perang.

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

Jerman tidak sepenuhnya tanpa kemampuannya sendiri dalam perang informasi. Jerman memotong kabel darat dan bawah laut Rusia yang menghubungkannya dengan sekutunya di Barat, dan beberapa kabel transatlantik yang diandalkan Inggris, serta mempelopori penggunaan kapal selam untuk melakukannya.[33] Mengingat redundansi jaringan Inggris, upaya-upaya ini pada akhirnya kurang efektif dari yang diharapkan Jerman. Yang terbukti jauh lebih berpengaruh adalah penggunaan intelijen radio Jerman melawan Rusia dalam Pertempuran Tannenberg pada bulan Agustus 1914, bulan pertama perang, yang memicu kekalahan telak bagi Rusia. Seorang perwira intelijen Jerman pada saat itu menyebut insiden tersebut sebagai "yang pertama dalam sejarah manusia saat intersepsi lalu lintas radio musuh memainkan peran penting."[34]

Pertempuran ini terjadi di tengah kemenangan Rusia di Front Timur. Ketika Rusia memasuki wilayah Prusia Timur, militernya menghadapi tantangan komunikasi yang signifikan dan menyebabkan kekalahan telak bagi Rusia. Pasukan Jerman yang kembali telah memotong jalur telegraf mereka sendiri, dan pasukan Rusia tidak memiliki cukup personel yang terlatih untuk mengatur komunikasi kabel di seluruh formasi mereka yang luas. Transmisi radio menyediakan alternatif, tetapi meski Rusia telah mengadopsi teknologi radio baru untuk komando dan kendali militer, mereka belum mengamankannya secara memadai. Kelompok yang berbeda telah ditugaskan untuk memecahkan sandi yang berbeda; sebagian besar hanya memiliki sedikit pelatihan untuk encoding dan decoding sinyal; sebagian kode diketahui telah dipecahkan oleh Inggris; dan buku tentang kode hanya terbatas atau tidak dapat dimengerti oleh banyak mereka.[35] Akibatnya, para komandan Rusia merasa mereka harus mengambil risiko dengan menggunakan pesan radio tanpa kode dan berharap Jerman tidak memantau mereka dengan hati-hati.

Namun, Jerman memantau sinyal dengan ketat. Setelah mengamati ketidakdisiplinkan radio Rusia dalam perang melawan Jepang, Jerman tahu bahwa transmisi Rusia yang tidak berkode bukanlah bagian dari upaya pengelabuan. Jerman kemudian menggunakan pengetahuan mereka terkait komunikasi langsung Rusia untuk menghilangkan "kabut perang" dan dengan yakin mengalahkan kekuatan yang lebih unggul. Rusia kehilangan seluruh tentaranya, dengan lebih dari 100.000 korban dan 92.000 tahanan dibandingkan Jerman dengan hanya 13.000 korban.

5. Inggris dalam Perang Dunia II: Batasan enkripsi

Rotor mekanis dari mesin sandi Lorenz dianggap tidak dapat dipecahkan secara efektif selama Perang Dunia II. Berbagai upaya Inggris untuk memecahkan kode tersebut memberi para pejabat akses ke komunikasi tingkat tinggi Jerman.

Sumber: Matt Crypto / Wikimedia Commons[36]

Penemuan telegrafi dan radio nirkabel membawa kenyamanan yang lebih besar, dibandingkan dengan kabel fisik, tetapi membawa risiko intersepsi yang lebih besar. Dalam Perang Dunia I dan II, kekuatan besar terdapat di dunia yang menganggap komunikasi radio dapat diakses oleh pihak lain. Di dunia semacam itu — tidak jauh berbeda dengan asumsi saat ini terkait kerentanan komputer dan sistem telekomunikasi modern — enkripsi dianggap penting untuk keamanan. Hasilnya, seperti yang dikatakan oleh sejarawan militer Amerika, adalah "pergulatan antara ahli kriptografi dan kriptanalis".[37] Ketika kekuatan besar berada di pihak yang salah dalam pegulatan tersebut, akibatnya dapat sangat membahayakan.

Untuk mencegah hal tersebut, organisasi akan menggunakan sandi untuk mengurangi risiko intersepsi yang membahayakan keamanan. Mereka juga melakukan "disiplin radio" untuk mencegah musuh mendapatkan wawasan tentang pola penggunaan melalui analisis lalu lintas radio.

Sebagian besar kekuatan besar diinvestasikan dalam upaya berskala industri yang sesungguhnya untuk mempelajari lalu lintas informasi musuh dan, jika memungkinan, untuk memecahkan kode musuh. Inggris Raya jauh lebih terpusat dalam analisis tentang musuhnya daripada Jerman, yang menyebarkan fungsi tersebut ke beberapa lembaga. Sama halnya dengan keberhasilan Inggris dalam intelijen sinyal dan analisis kriptografi yang membentuk jalannya Perang Dunia I, mereka juga

membentuk jalannya Perang Dunia II ketika operasi Inggris di Bletchley Park memecahkan kode Enigma dan Lorenz Jerman.

Sistem kode Enigma dan Lorenz menggunakan mesin rotor yang luar biasa kompleks untuk mengenkripsi pesan-pesan yang diyakini Jerman "akan tetap aman".[38] Setiap penekanan tombol akan mengganti karakter dengan karakter lain berdasarkan pengaturan unik mesin, dan pengaturan tersebut — yang, untuk sistem Lorenz, melebihi jumlah total atom di alam semesta — perlu dibagikan oleh pengirim dan penerima untuk membaca pesannya.[39] Enigma digunakan oleh militer, Gestapo, dan diplomat; Lorenz, yang bahkan lebih kompleks, digunakan oleh Adolf Hitler dan pejabat senior Nazi dan militer untuk berkomunikasi dengan satu sama lain.

Keberhasilan Inggris dalam memecahkan Enigma dan Lorenz adalah berkat beberapa faktor. Pertama, berkat kerja sama intelijen sekutu dengan Polandia, yang telah mengeksploitasi beberapa kesalahan Jerman untuk memecahkan beberapa mesin Enigma yang lebih sederhana.[40] Seperti yang dikatakan oleh seorang kriptanalis Inggris pada waktu itu, upaya mereka "tidak akan pernah berhasil" tanpa kontribusi Polandia.[41]

Kedua, karena Jerman terlalu percaya diri dan tidak pernah curiga jika kode mereka telah dipecahkan dan karenanya melupakan perubahan yang cukup mudah yang akan memaksa Inggris untuk memulai ulang segalanya.[42] Walaupun demikian, keyakinan Jerman terhadap keamanan mesinnya "hampir benar", kata seorang pejabat senior Bletchley Park.[43]

Terakhir, karena satu kesalahan besar dalam "disiplin radio" Jerman yang menciptakan celah untuk merekayasa ulang sistem penyandian Jerman meski belum pernah melihatnya secara langsung.[44] Bahkan sistem yang paling canggih pun rentan terhadap kesalahan pengguna, dan musuh yang waspada dapat mengeksploitasi sistem tersebut.

Dengan memecahkan Enigma dan Lorenz, Inggri Raya telah memiliki akses ke beberapa komunikasi Jerman yang paling sensitif. Winston Churchill dilaporkan memuji intelijen tersebut sebagai alasan utama Inggris Raya memenangkan perang, dan Dwight D. Eisenhower dilaporkan menyebutnya "pasti".[45] Sejarawan resmi intelijen Inggris, Sir Francis Harry Hinsely, berpendapat bahwa keberhasilan ini "mempersingkat perang hingga tidak kurang dari dua tahun dan mungkin hingga empat tahun", melemahkan Field Marshall Erwin Rommel di Afrika, membalikkan kerugian pengiriman sekutu ke U-Boot Jerman, dan memungkinkan pendaratan Normandia.[46] Intelijen tersebut juga mengizinkan Inggris untuk mengidentifikasi hampir semua mata-mata Jerman yang memasuki negara dan sering kali mengubahnya atau menggunakannya untuk mengembalikan intelijen yang salah, dengan kepala program mencatat bahwa intelijen Inggris "secara aktif menjalankan dan mengendalikan sistem spionase Jerman di negara ini".[47] Hanya sedikit negara yang pernah memiliki pengetahuan mendalam tentang negara lain selama masa perang.

Secara keseluruhan, keberhasilan upaya Inggris melawan Jerman, pemantauan Polandia selama masa damai atas komunikasi Jerman, dan keputusannya untuk membagikan terobosannya dengan Inggris Raya, memiliki pelajaran yang dapat diterapkan ke persoalan saat ini ketika kekuatan besar melakukan pengintaian cyber terhadap satu sama lain. Lebih luas lagi, mereka yang menyarankan enkripsi untuk mengurangi masalah akses musuh ke jaringan telekomunikasi mungkin membuat kesalahan yang tidak berbeda dengan yang pernah dibuat Jerman sendiri: keyakinan yang berlebihan pada teknologi dan perhatian yang terbatas pada kemungkinan kesalahan manusia yang selalu ada.

6. Operasi Ivy Bells: Kedalaman pengejaran informasi

USS Halibut, yang dilaporkan terlibat dalam upaya penyadapan saluran telepon bawah laut Soviet.

Sumber: Angkatan Laut AS / Wikimedia Commons[48]

Uni Soviet jauh lebih memperhatikan enkripsinya daripada Nazi, yang mengandalkan versi Enigma mereka sendiri — yang dikenal sebagai Fialka — yang secara substansial lebih kompleks.[49] Karena alasan itu, berbagai kumpulan intelijen strategis yang dibuat saat Perang Dunia II setelah kode Jerman dipecahkan tidak memiliki analog yang diketahui secara publik saat Perang Dingin. Mengingat tantangan ini, metode lain untuk menembus telekomunikasi musuh pun dirintis. Salah satu upaya yang paling berani dilakukan berhubungan dengan kabel bawah laut.

Awal mula diciptakannya kabel bawah laut pada abad ke-19 pada akhirnya menyebabkan upaya pemotongan dan terkadang penyadapan, sering kali di perairan yang lebih dangkal atau di darat yang lebih mudah dilakukan. Sebaliknya, melakukan operasi di perairan dalam yang dikendalikan oleh musuh dianggap hampir tidak mungkin, terutama jika dilakukan secara diam-diam. Dimulai pada abad ke-20, Inggris dan kekuatan besar berikutnya telah mencapai keputusan tentang keamanan kabel bawah laut: jika lokasi pendaratan diamankan, dan kabel tidak melintasi negara netral atau negara yang tidak bersahabat, mereka umumnya akan aman dari intersepsi dan sering kali aman dari pemotongan, terutama pada masa damai.[50]

Namun, selama Perang Dingin, hal tersebut berubah. Kehadiran kapal selam nuklir menghadirkan kemungkinan penyadapan kabel bawah laut di perairan yang lebih dalam. Namun, mengirim penyelam untuk mengakses kabel di dasar laut yang dalam dianggap lebih mirip dengan eksplorasi ruang angkasa daripada upaya manipulasi kabel yang biasa dilakukan pada era sebelumnya. Melakukan penyadapan dalam kondisi seperti itu juga menantang secara teknis.

Ketika Amerika Serikat mencurigai bahwa kabel bawah laut Soviet mungkin melewati markas angkatan laut di Vladivostok hingga ke pangkalan kapal selam di semenanjung Kamchatka, Amerika berusaha mengatasi rintangan ini, menunjukkan nilai dari intelijen sinyal.[51] Menyadap kabel berukuran lima inci tersebut diyakini akan memberikan informasi penting tentang kekuatan nuklir Soviet.[52] Sementara Soviet mengenkripsi semua lalu lintas informasi yang dikirim melalui udara, Amerika Serikat berharap Soviet akan menganggap lalu lintas melalui kabel bawah laut yang dilindungi hampir tidak mungkin untuk diakses, dan oleh karena itu tidak akan mengenkripsinya. Selain itu, "Laksamana dan jenderal Soviet akan menjadi terlalu angkuh dan tidak sabar untuk menghadapi lautan kriptografer yang sudah kewalahan oleh sebagian besar pekerjaan mereka", dan akan bersikeras untuk melakukan komunikasi suara tanpa keamanan.[53] Penyadapan kemudian akan memberikan harta intelijen yang berharga, dan Angkatan Laut AS meluncurkan Operasi Ivy Bells untuk membangunnya.

Banyak hasil penyadapan dan intelijen yang diperoleh tetap dirahasiakan, tetapi sumber terbuka memberikan beberapa detail tentang operasi yang unik dan inovatif tersebut. Amerika Serikat mengirim kapal selam nuklir, USS Halibut, untuk secara diam-diam menyelinap melewati angkatan laut Soviet dan menemukan kabel bawah laut di area seluas 600.000 mil persegi.[54] Teknologi inovatif diciptakan untuk memastikan bahwa penyelam dapat bekerja di bawah tekanan yang besar dan dalam suhu yang sangat dingin selama beberapa jam. Demikian pula, metode baru untuk melakukan penyadapan di lingkungan yang menantang ini telah dirancang.[55] Semua ini harus dilakukan tanpa mengundang kecurigaan atau deteksi Soviet. Jika kapal terdeteksi, Soviet mungkin akan menaikinya atau menghancurkannya.

Operasi tersebut akhirnya terbukti berhasil, dan sepanjang tahun 1970-an, Angkatan Laut AS menyadap dan merekam pesan tanpa keamanan dari seluruh kabel. Setiap beberapa bulan, kapal selam Amerika secara diam-diam menyelinap ke perairan Soviet, menghindari serangan kapal selam, mengerahkan penyelam ke jalur kabel yang disadap, dan mengambil rekaman komunikasi Soviet — menghasilkan potongan intelijen yang sangat berharga dan langka. Ketika Amerika Serikat telah memperluas "jaringan satelit mata-mata, pesawat, stasiun pendengar, dan kapal selam" untuk mengumpulkan sinyal intelijen, mereka "tidak dapat menembus saluran telepon yang terpasang" di dalam wilayah musuh. Upaya ini menggambarkan pergeseran evolusioner dalam bidang telekomunikasi, yaitu bahwa data dan sinyal yang ditransmisikan melalui media apa pun dan dengan cara apa pun dapat diakses oleh aktor dengan tekad dan alat yang tepat. Meski penyadapan ini pada akhirnya terancam akibat kebocoran, penyadapan telekomunikasi yang dilakukan memberikan intelijen militer dan politik yang berharga bagi Amerika Serikat dan sekutunya.[56]

Persaingan telekomunikasi modern dalam perspektif sejarah

Pada akhir Perang Dingin, Amerika Serikat dengan jelas telah menggantikan Inggris Raya sebagai hegemon informasi. Amerika Serikat mempertahankan posisinya di internet global, kemampuan ruang angkasa yang kuat, dominasi di sebagian besar teknologi internet, dan — menurut pengungkapan publik — kemampuan canggih untuk mencegat atau mungkin menolak komunikasi musuh.

Keunggulan Amerika ini sekarang sedang diuji, seperti Inggris Raya lebih dari seabad yang lalu. Rusia, dan khususnya Tiongkok, kini menantang dominasi AS. Ketika Amerika Serikat menikmati posisi penting dalam banyak aliran data, kekuatan lain makin berupaya untuk mengurangi ketergantungan mereka pada jaringan AS. Pada saat yang sama, posisi penting Amerika kurang diperlukan untuk intersepsi dibandingkan dengan Inggris Raya seabad yang lalu. Internet memungkinkan penyusupan tanpa kendali atas infrastruktur fisik. Smartphone dan jaringan komputer dapat diretas, dan apakah komunikasi sensitif seseorang terancam oleh penyadapan secara fisik seperti pada era sebelumnya atau oleh gangguan virtual pada era modern, hasil akhirnya tetap sama. Koneksi dengan cara ini kemungkinan besar menciptakan kerentanan yang lebih besar sekarang dibandingkan pada era telegraf atau radio nirkabel.

Rusia telah menjadi negara terdepan yang mengeksploitasi kerentanan tersebut. Pada tahun 2007, Rusia meluncurkan gelombang serangan cyber terhadap lembaga-lembaga Estonia, yang sebagian besar mendistribusikan serangan penolakan layanan.[57] Pada tahun 2008, Rusia meluncurkan serangan cyber pada saat Perang Rusia-Georgia. Ini tidak hanya melibatkan serangan penolakan layanan yang terarah, tetapi juga upaya untuk mengarahkan ulang situs web pemerintah, mengambil alih server pemerintah Georgia, dan mengubah rute lalu lintas internet Georgia melalui server yang dikendalikan Rusia — dengan beberapa serangan dilakukan sebelum konflik bertepatan dengan aksi militer Rusia.[58] Pada tahun 2014, ketika Rusia menyerang Krimea, Rusia menggabungkan serangan cyber dengan kendali fisik jaringan telekomunikasi. Tentara Rusia menyita fasilitas telekomunikasi Ukraina, menggunakannya untuk memutus komunikasi di Krimea dan bahkan untuk melakukan serangan cyber serta gangguan di bagian lain Ukraina.[59] Pada tahun 2015, Rusia memulai gelombang serangan cyber terhadap infrastruktur Ukraina, yang mematikan listrik bagi ratusan ribu warga Ukraina dalam dua kejadian. Selama beberapa tahun berikutnya, Rusia terus meluncurkan gelombang serangan yang belum pernah dilakukan sebelumnya di seluruh Ukraina yang mencakup “media, keuangan, transportasi, militer, politik, dan energi” — hampir setiap segmen masyarakat Ukraina — yang diyakini sebagian orang sebagai upaya pelatihan untuk melawan Amerika Serikat.[60] Pada saat yang sama, Rusia melanjutkan berbagai serangan di seluruh Baltik dan terkenal berupaya membentuk pemilu AS pada tahun 2016 dan 2020 dengan kampanye disinformasi, serta di negara lainnya.[61] Pada tahun 2021, pemerintah AS secara resmi menuduh Rusia melakukan peretasan perusahaan IT SolarWinds, serangan canggih yang membahayakan sebagian besar pemerintah federal dan beberapa perusahaan besar AS.[62]

Tiongkok merupakan kekuatan besar lainnya yang melakukan investasi signifikan dalam persaingan telekomunikasi, meski tidak seperti Rusia, upaya Tiongkok tidak hanya untuk mengeksploitasi infrastruktur internet yang ada, tetapi juga untuk membangun jaringan dan infrastruktur yang dapat dipengaruhi dan bahkan dikendalikannya. Seperti Rusia, Tiongkok telah

mahir mengeksploitasi kerentanan internet yang ada. Pada awal 2000-an, Tiongkok meluncurkan gelombang serangan terhadap jaringan Departemen Pertahanan AS dengan apa yang disebut sebagai Operation Titan Rain.[63] Pemerintahan di seluruh dunia — Amerika Serikat, Inggris Raya, Prancis, Jerman, Kanada, Australia, Jepang, Korea Selatan, Taiwan, India, dan lainnya — telah mengeluhkan gangguan Tiongkok dalam jaringan pemerintahan mereka. Beberapa serangan cyber terbesar dalam dekade terakhir dikonfirmasi oleh Jaksa Agung AS William Barr telah dilakukan oleh agen Tiongkok, antara lain termasuk pencurian catatan dari Kantor Manajemen Personalia AS (catatan 21 juta orang), hotel Marriott (400 juta), asuransi kesehatan Anthem (80 juta), dan Equifax (147 juta).[64]

Pada saat yang sama, Tiongkok juga meletakkan fondasi untuk infrastruktur internet masa depan dan, mengingat upaya sebelumnya, tampaknya upaya ini tidak bersifat komersial sekarang atau akan tetap murni bersifat komersial pada masa mendatang. Investasi Tiongkok paling menonjol dalam jaringan 5G diharapkan dapat membentuk fondasi untuk ekonomi yang lebih cerdas dan terhubung yang menghubungkan perangkat dan sensor yang tak terhitung jumlahnya. Bersemangat untuk membangun jaringan ini di seluruh dunia, Tiongkok telah mensubsidi berbagai perusahaan dan proyek 5G terdepan di seluruh dunia sebagai bagian dari inisiatif Digital Silk Road. Dengan harga yang kompetitif, perusahaan seperti Huawei mampu mengungguli vendor 5G utama lainnya dan menguasai pangsa pasar global yang signifikan, dan menjadikan Tiongkok sebagai pemimpin dalam pembangunan jaringan ini. Selain 5G, pemerintah Tiongkok telah mensubsidi upaya untuk membangun infrastruktur internet atau komunikasi di hampir semua benua. Semua upaya ini dilengkapi dengan kampanye untuk membentuk standar global, prioritas kebijakan utama Tiongkok yang diabadikan dalam dokumen perencanaan tingkat tinggi yang — seperti dalam persaingan Anglo-Jerman melalui radio seabad yang lalu — dapat membentuk masa depan telekomunikasi dengan cara yang menguntungkan Tiongkok. Untuk itu, Tiongkok baru saja meluncurkan inisiatif keamanan data yang baru.[65]

Beberapa pihak khawatir jika aktivitas Tiongkok akan membuka kemungkinan bahwa Beijing akan memiliki kendali de facto atas jaringan ini, entah untuk mencegat lalu lintas atau menolak akses. Sedikit informasi publik yang tersedia tentang upaya Tiongkok untuk memperoleh kendali tersebut, tetapi pemerintah AS mengungkapkan pada Februari 2020 bahwa Huawei memiliki pintu belakang di peralatan jaringannya, dan tidak mengungkapkannya kepada perusahaan terkait yang dikontraknya, serta bahwa pintu belakang tersebut melampaui yang terkadang diminta oleh pemerintah negaranya sebagai bagian dari penyadapan yang sah.[66] Selain itu, pelaporan publik telah mengungkapkan bahwa Huawei membantu pemerintah seperti Uganda dan Zambia dengan mengorbankan identitas para pihak yang tidak bersepakat.[67] Bahkan di luar kasus Huawei, sebuah perusahaan keamanan cyber baru-baru ini menemukan pintu belakang dalam perangkat lunak pajak yang wajib diinstal oleh perusahaan asing menurut instruksi pemerintah Tiongkok.[68] Terlepas dari apakah kasus-kasus ini menunjukkan bahwa Huawei sendiri telah mengeksploitasi posisinya atas jaringan ini, perilaku perusahaan dan rekam jejak Tiongkok atas serangan cyber dan spionase, adalah alasan yang harus diperhatikan.

Alasan utama lainnya untuk diperhatikan berasal dari sejarah dan perilaku kekuatan besar yang lebih liberal yang lebih terkekang oleh aturan hukum. Memang, kasus-kasus sejarah sebelumnya sangat menunjukkan bahwa jenis kekuasaan dan pengaruh yang akan dimiliki perusahaan seperti Huawei kemungkinan besar akan dieksploitasi oleh pemerintah Tiongkok, sama seperti kekuatan

besar lainnya yang sering mengeksploitasi posisi perusahaan atau kemampuan mereka di bidang telekomunikasi.

Dari perspektif sejarah yang lebih luas tersebut, bukti tersebut dapat mengarahkan banyak pengamat untuk menyimpulkan bahwa peran Huawei dalam jaringan telekomunikasi perlu diwaspadai — bahkan jika motif perusahaan memang murni bersifat komersial, janji "no backdoors and no spying" dapat dipercaya, dan Beijing tulus dalam komitmennya untuk menghormati janji tersebut.

Secara lebih luas lagi, seperti yang dijelaskan dalam laporan ini, banyak elemen persaingan kekuatan telekomunikasi yang dianggap baru saat ini memiliki akar di masa lalu. Sepanjang sejarah, beberapa tema telah terulang:

- *Kekuatan:* Kendali atas jaringan telekomunikasi telah menjadi bentuk kekuatan politik sejak diciptakan lebih dari 150 tahun yang lalu. Inggris Raya mengeksploitasi perannya dalam bidang telekomunikasi dan radio, Amerika Serikat kemungkinan besar telah melakukannya pada era internet modern, dan terdapat alasan untuk mengkhawatirkan kemungkinan Tiongkok akan mencoba melakukannya pada saat ini.

- *Rasa Puas Diri*: Masa damai dan kesejahteraan yang lama menyebabkan rasa puas diri terhadap risiko telekomunikasi. Pada abad ke-19, kekuatan besar sangat bergantung pada perusahaan asing dan jaringan yang dioperasikannya, seperti negara-negara saat ini yang bersedia menerima peralatan dan operasi telekomunikasi Tiongkok. Namun pada akhirnya, ketergantungan pada pesaing atau musuh potensial terbukti menjadi bencana bagi negara-negara seperti Jerman dan membentuk ulang politik dunia.

- *Eksploitasi:* Teknologi telekomunikasi baru selalu mengarah pada upaya baru untuk mencegat, menolak, atau mengeksploitasinya. Terlepas dari harapan bahwa enkripsi dapat mempersulit upaya Tiongkok untuk mencegat komunikasi modern, harapan periode sebelumnya terhadap enkripsi dihancurkan oleh kesalahan pengguna dan upaya negara saingan untuk memecahkannya, seperti yang terjadi pada Jerman ketika Inggris Raya memecahkan kode yang seharusnya "tidak dapat dipecahkan". Kerendahan hati harus menyertai setiap gelombang teknologi yang seharusnya aman.

- *Kemenangan:* Negara sering kali mengembangkan teknologi telekomunikasi mereka sendiri, terutama ketika ketegangan kekuatan besar meningkat. Pemerintah Tiongkok bangga akan pencapaian Huawei, dan memperjuangkannya di seluruh dunia — bahkan mengancam negara yang menolak teknologinya. Tidak biasa bagi perusahaan yang begitu dekat dengan pemerintah negara asalnya untuk kebal dari tekanan negara ketika begitu banyak juara telekomunikasi lain di sepanjang sejarah juga tidak.

- *Standar*: Standar telekomunikasi dapat menentukan siapa yang memegang kekuatan jaringan, seperti Jerman yang memanfaatkan badan penetapan standar untuk mematahkan dominasi Inggris Raya dalam radio nirkabel. Saat ini, persaingan tersebut sedang

berlangsung di badan-badan seperti International Telecommunications Union, dan peran Huawei di dalamnya menunjukkan perlunya mempertimbangkan apakah standarnya akan memungkinkan Tiongkok untuk membentuk ulang telekomunikasi.

- *Penolakan:* Keamanan jaringan tidak hanya tentang intersepsi dan keamanan data, tetapi juga tentang penolakan operasi seluruh jaringan atau akses ke jaringan luar. Inggris Raya memutus Jerman dari jaringan telegraf dunia, dan peran Huawei dalam jaringan dapat memberdayakannya untuk mematikan jaringan di negara-negara yang menampung operasinya meski tidak dapat mengakses data dengan mudah.

- *Penentuan:* Banyak negara mengabaikan sejauh mana musuh dapat melakukan upaya luar biasa untuk membahayakan jaringan mereka, dan kemudian dikejutkan ketika hal itu terjadi. Kemampuan Inggris untuk memecahkan kode Jerman dalam Perang Dunia II melalui upaya berskala industri dan kemampuan Amerika untuk memanfaatkan kabel internal kapal selam Soviet yang seharusnya tidak dapat digunakan menunjukkan seberapa jauh cara yang akan digunakan oleh kekuatan besar untuk mengakses intelijen sinyal yang penting. Tiongkok juga cenderung melakukan upaya maksimal seperti ini, dan bahkan jika Huawei merasa sulit untuk mempersenjatai posisinya dalam jaringan modern, meremehkan kecerdasan dan dorongan pesaing yang gigih seperti Tiongkok adalah motif berulang dalam persaingan telekomunikasi.

Seperti yang diperlihatkan dalam laporan ini, banyak elemen dari persaingan kekuatan besar atas telekomunikasi yang tetap sama, meski para pemainnya mungkin berbeda.

Tentang Penulis

Rush Doshi adalah direktur Brookings China Strategy Initiative dan peneliti di Brookings Foreign Policy. Ia juga menjadi rekan peneliti di Paul Tsai China Center di Yale Law School dan anggota dari kelas perdana Wilson China fellows. Penelitiannya berfokus pada strategi besar Tiongkok serta masalah keamanan Indo-Pasifik. Doshi adalah penulis *The Long Game: China's Grand Strategy to Displace American Order*, yang akan diterbitkan oleh Oxford University Press. Saat ini dia bertugas di pemerintahan Biden.

Kevin McGuness baru-baru ini bekerja bersama Brookings sebagai ekstern dari Department of Defense Skillbridge Program, tempat dia banyak berkontribusi dalam berbagai proyek di Center for East Asia Policy Studies. Dia adalah veteran Angkatan Udara dan baru saja menyelesaikan tugasnya sebagai staf pengajar di United States Air Force Academy, dan bertugas memberikan kuliah untuk jurusan hubungan internasional dan politik Asia. Dia juga bekerja sebagai asisten riset di Institute for National Strategic Studies' Center for the Study of Chinese Military Affairs dan berfokus pada modernisasi dan keamanan PLA di Indo-Pasifik.

Ucapan Terima Kasih

Para penulis ingin mengucapkan terima kasih kepada para mantan pekerja magang Isabella Lu, Zijin Zhou, dan Gaoqi Zhang atas bantuan penelitian mereka dalam proyek ini, beberapa pengulas anonim, Claire Harrison dan Ted Reinert atas penyuntingan laporan ini, serta Chris Krupinski dan Rachel Slattery atas penyediaan tata letak dan desain web. Brookings berterima kasih kepada Departemen Luar Negeri AS dan Institute for War and Peace Reporting atas dana penelitian yang diberikan.

Laporan ini diselesaikan sebelum Rush Doshi menjabat di pemerintahan, hanya melibatkan sumber-sumber terbuka, dan tidak serta merta mencerminkan kebijakan resmi atau posisi lembaga pemerintah AS mana pun.

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

Factor Into Huawei 5G Decision," Time, 19 Desember, 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), chapter 1. Daniel R. Headrick, The Invisible Weapon: Telecommunications and International Politics, 1851-1945 (Oxford, Inggris: Oxford University Press, 1991), bab 1.
[3] Ibid., menurut pengamatan Headrick.
[4] Ibid.
[5] Ibid.
[6] Ibid., menurut pengamatan Headrick.
[7] Heidi Tworek, *News from Germany: The Competition to Control World Communications, 1900-1945* (New York: Harvard Historical Studies, 2019). 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. 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., chapter 5. Ibid., bab 5.
[11] Jonathan Winkler, "Information Warfare in World War I," *The Journal of Military History* 73, no. 3 (2009): 845–67, https://doi.org/10.1353/jmh.0.0324. Jonathan Winkler, "Information Warfare in World War I," 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," *The Century Illustrated Monthly Magazine* 57 (1899): 708-717, https://books.google.com/books?id=Y7fPAAAAMAAJ&pg=PA708#v=onepage&q&f=false. 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, November 6, 2015, https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/; Jonathan Winkler, "Silencing the Enemy: Cable-Cutting in the Spanish–American War," War on the Rocks, 6 November 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."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."Winkler, "Silencing the Enemy."
[17] Library of Congress, George Grantham Bain Collection, https://www.loc.gov/pictures/item/2014683102/.
[18] Walaupun demikian, Heidi Tworek menyatakan bahwa perannya sendiri sering kali dibesar-besarkan dalam perkembangan teknologi ini. Heidi Tworek, *News from Germany.*
[19] Marc Raboy, "The First Company That Wanted to 'Connect the World' Wasn't Google or Facebook," Media@LSE, August 24, 2016, https://blogs.lse.ac.uk/medialse/2016/08/24/the-first-company-that-wanted-to-connect-the-world-wasnt-google-or-facebook/. Marc Raboy, "The First Company That Wanted to 'Connect the World' Wasn't Google or Facebook," Media@LSE, 24 Agustus 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.Tworek, *News from Germany*, 12–13.
[21] Michael Friedewald, "Telefunken vs. Marconi, or the Race for Wireless Telegraphy at Sea, 1896-1914," SSRN (January 9, 2014): https://doi.org/10.2139/ssrn.2375755. Michael Friedewald, "Telefunken vs. Marconi, or the Race for Wireless Telegraphy at Sea, 1896-1914," SSRN (9 Januari 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. Marc Raboy, Marconi: The Man Who Networked the World (Oxford, Inggris: Oxford University Press, 2016), 226–28.

[24] Misalnya, Telefunken pun bahkan aktif di berbagai wilayah yang tidak banyak memiliki kehadiran kolonial Jerman, seperti Amerika Latin.
[25] George Johnson, ed., *The All Red Line: The Annals and Aims of the Pacific Cable Project* (Ottawa: James Hope and Sons, 1903), 10, di 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, December 15, 2017, https://www.bbc.com/news/world-europe-42367551. Gordon Corera, "How Britain Pioneered Cable-Cutting in World War One," BBC News, 15 Desember 2017, https://www.bbc.com/news/world-europe-42367551.
[27] Jonathan Winkler, "Information Warfare in World War I," 847.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. 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.Winkler, "Information Warfare in World War I," 849.
[30] Ibid., 851. Ibid., 851.
[31] Gordon Corera, "Why Was the Zimmermann Telegram so Important?," BBC News, January 17, 2017, https://www.bbc.com/news/uk-38581861; Patrick Beesly, *Room 40: British Naval Intelligence 1914-18* (San Diego: Harcourt Brace Jovanovich, 1982). Gordon Corera, "Why Was the Zimmermann Telegram so Important?," BBC News, 17 Januari 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 dan Valdemar Langlet, *Det stora världskriget* [The Great World War] (1915), di Wikimedia Commons, https://commons.wikimedia.org/wiki/File:German_WW_I_field_telegraph_002.jpg.
[33] Jonathan Winkler, "Information Warfare in World War I."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/. 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). Bruce Norman, Secret Warfare: The Battle of Codes and Ciphers (Newton Abbot, Inggris: David & Charles Ltd, 1973); Prit Buttar, Collision of Empires: The War on the Eastern Front in 1914 (Oxford, Inggris: Osprey Publishing, 2014).
[36] Matt Crypto, "The rotors of a Lorenz SZ42 cipher machine on display at Bletchley Park museum," di 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. "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" (seminar, Cambridge, Inggris, 19 Oktober 1993), http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF. Cambridge, U.K., October 19, 1993), http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF.
[39] $1x10^{170}$ kemungkinan pengaturan.
[40] "Bletchley Park Remembers Polish Code Breakers," BBC News, July 14, 2011, https://www.bbc.com/news/uk-england-beds-bucks-herts-14141406. "Bletchley Park Remembers Polish Code Breakers," BBC News, 14 Juli 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). Gordon Welchman, The Hut Six Story: Breaking the Enigma Codes (Cleobury Mortimer, Inggris: Classic Crypto Books, 1997).
[42] Harry Hinsley, "The Influence of ULTRA."Hinsley, "The Influence of ULTRA."
[43] Ibid. Ibid.

[44] Lihat, sebagai contoh , Jerry Roberts, Lorenz: Breaking Hitler's Top Secret Code at Bletchley Park (Cheltenham, Inggris: History Press, 2017).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. F. W. Winterbotham, The Ultra Secret (New York: Harper & Row, 1974), 154, 191.
[46] Harry Hinsley, "The Influence of ULTRA." Hinsley, "The Influence of ULTRA."
[47] Calder Walton, "The Spies Who Came In From the Continent," *Foreign Policy*, April 27, 2019, https://foreignpolicy.com/2019/04/27/the-spies-who-came-in-from-the-continent-espionage-britain-brexit/. Calder Walton, "The Spies Who Came In From the Continent," Foreign Policy, 27 April 2019, https://foreignpolicy.com/2019/04/27/the-spies-who-came-in-from-the-continent-espionage-britain-brexit/.
[48] Angkatan Laut AS, di Wikimedia Commons, https://commons.wikimedia.org/wiki/File:USS_Halibut_with_bow_thruster.jpg.
[49] Anna Borshchevskaya, "The Soviets' Unbreakable Code," *Foreign Policy*, April 27, 2019, https://foreignpolicy.com/2019/04/27/the-soviets-unbreakable-code-fialka-encryption-espionage-russia-kgb-spy/. Anna Borshchevskaya, "The Soviets' Unbreakable Code," Foreign Policy, 27 April 2019, https://foreignpolicy.com/2019/04/27/the-soviets-unbreakable-code-fialka-encryption-espionage-russia-kgb-spy/.
[50] Daniel R. Headrick, The Invisible Weapon, bab 4. Headrick, *The Invisible Weapon*, chapter 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. Sherry Sontag, Christopher Drew, dan 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. 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*, March 30, 2017, https://www.popularmechanics.com/technology/security/a25857/operation-ivy-bells-underwater-wiretapping/.Matt Blitz, "Navy Divers and Their Daredevil Mission to Spy on the Soviet Union at the Bottom of the Sea," Popular Mechanics, 30 Maret 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." 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, April 27, 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/. Damien McGuinness, "How a Cyber Attack Transformed Estonia," BBC News, 27 April 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, January 6, 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, no. 1 (2012): 3–24, https://journals.sagepub.com/doi/10.1177/0967010611431079. David Hollis, "Cyberwar Case Study: Georgia 2008," Small Wars Journal, 6 Januari 2011, https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008; Ronald J. Deibert, Rafal Rohozinski, dan Masashi Crete-Nishihata, "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war," Security Dialogue 43, no. 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, March 4, 2014, https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-

blocked-idUSBREA231R220140304 Pavel Polityuk dan Jim Finkle, "Ukraine Says Communications Hit, MPs Phones Blocked," Reuters, 4 Maret 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 Mei 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*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/ Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," Wired, 20 Juni 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," Departemen Kehakiman Amerika Serikat, 19 Oktober 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, June 28, 2017), https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/. Constanze Stelzenmüller, "The impact of Russian interference on Germany's 2017 elections," (kesaksian kongres, 28 Juni, 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 Januari 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. "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*, February 11, 2020, https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/. Garrett Graff, "China's Hacking Spree Will Have a Decades-Long Fallout," Wired, 11 Februari 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 September 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*, February 12, 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256. Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," The Wall Street Journal, 12 Februari 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*, August 15, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017. Joe Parkinson, Nicholas Bariyo, dan Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," The Wall Street Journal, 15 Agustus 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, June 25, 2020, https://www.bloomberg.com/news/articles/2020-06-25/hidden-back-door-embedded-in-chinese-tax-software-firm-says. William Turton, "Hidden Back Door Embedded in Chinese Tax Software, Firm Says," Bloomberg, 25 Juni 2020, https://www.bloomberg.com/news/articles/2020-06-25/hidden-back-door-embedded-in-chinese-tax-software-firm-says.