SECURITY, STRATEGY, AND ORDER

MARCH 2021

HUAWEI MEETS HISTORY

GREAT POWERS AND TELECOMMUNICATIONS RISK, 1840-2021

RUSH DOSHI AND KEVIN MCGUINESS

B | Foreign Policy
at BROOKINGS

HUAWEI MEETS HISTORY
GREAT POWERS AND TELECOMMUNICATIONS RISK, 1840-2021

RUSH DOSHI AND KEVIN MCGUINESS

EXECUTIVE SUMMARY

In late 2018, amid American concerns about whether Canada would welcome Huawei into its telecommunications networks, Canadian Prime Minister Justin Trudeau made a series of statements that captured conventional wisdom across much of the world. “It shouldn’t be a political decision,” he declared at the time, and Canada would not “let politics slip into decisions” about Huawei’s role in its network.[1]

The notion that power politics could be removed from questions over telecommunications was not only optimistic, it was also out of step with the history of telecommunications. This report explores that history, and it shows how power and telecommunications have almost always been closely linked. When states ignored those linkages and were cavalier with the security of their own networks, the results were disadvantageous and at times even disastrous.

This report examines several major cases of great power competition in telecommunications dating back to the earliest inception of electrical telecommunications in the 1840s. These cases demonstrate that many of the questions policymakers confront today have close analogues to the past. While the present debate over network security and 5G infrastructure may feel new, it in fact echoes forgotten disputes dating back to the dawn of electrical telecommunications some 150 years ago. Moreover, many of the familiar elements of telecommunications competition today — such as the use of standard-setting bodies, state subsidies, cable taps, information warfare, developing country markets, and encryption to gain advantage — were developed more than a century ago, with important lessons for present debates.

A list of these key lessons is provided below:

1. **Control over global telecommunications networks is a form of political power.** 5G networks are expected to form the foundation of a smarter, connected economy linking countless devices and sensors together. Eager to build these networks worldwide, China has subsidized its 5G champion companies and projects around

the world as part of a "Digital Silk Road" initiative. That effort is analogous to Great Britain's pursuit of network dominance at the dawn of electrical telegraphy. Britain built its advantage over six decades by steadily increasing the dependence of other states on its networks — even forgoing fees and economic benefits to entice them to run cables through Britain — while also reducing Britain's dependence on foreign networks. It eventually controlled more than half of the world's cable traffic, the largest radio network, and the largest fleet of cable ships. Britain's "information hegemony" allowed it to cut Germany off from virtually all global telecommunications in World War I and forced Berlin to route traffic over British-owned lines susceptible to British monitoring, which later proved decisive in Germany's defeat in the conflict.

2. **Long periods of peace and prosperity generally lead to complacency about telecommunications risks.** In the last 30 years, post-Cold War peace and economic globalization coincided with rapid progress in telecommunications that led states to prioritize revolutionary commercial benefits over political and security risks, including even foreign ownership or operation of networks. A similar development took place at the dawn of telecommunications in the 1840s, which also coincided with a period of relative peace and globalization that continued until World War I. For much of that era, the desire to capture the seemingly miraculous commercial potential of new communications technologies obscured questions related to reliance on foreign networks or companies. Great Britain benefited from the complacency of others by building and then exploiting an unassailable nodal position in global networks, with most other great powers dependent on its networks.

3. **When states are complacent about their telecommunications security, the results can be disastrous and reshape world politics.** Decades of German complacency about its dependence on British telecommunications lines meant that by the time Berlin awakened to the risks of that dependency, it was too late to change it. When World War I broke out, Britain cut all of Germany's cables and forced Berlin to route traffic through British networks despite the risk of interception, which led to the uncovering of the "Zimmerman telegram," which helped bring the United States into the war. Similarly, Russian indiscipline in wireless radio transmissions in World War I allowed the Germans to intercept communications, "see" the movement of Russian troops in real time, and deal them a decisive defeat at the Battle of Tannenberg. Then, in World War II, Nazi overconfidence in its ciphers led to minimal efforts to update them, allowing Great Britain to break the codes and obtain intelligence that is believed to have shortened the war by two to four years. Given the power of information, even occasional bouts of signals indiscipline or complacency can alter history.

4. **New technology always leads to new efforts to intercept it.** The emergence of undersea cables led to efforts to cut and tap those lines as early as the Spanish-American War; radio transmission gave rise to efforts by rivals to capture network nodes and to intercept transmissions; and the emergence of sophisticated ciphers for encryption produced industrial-scale efforts to break them. In each era, some believed a new leap in communications might be less vulnerable than the ones that preceded it. Each time, however, the cycle of innovation and exploitation continued.

5. **Telecommunications networks have never been politically neutral, particularly in times of tension.** In 2019, Huawei executives made a "no-backdoor, no-spying" pledge and promised that their company would remain outside of politics, with China's government committing to respect the pledge. But even more than a century ago,

telecommunications companies and their host governments made similar promises publicly while privately breaking them and working together in both peacetime and wartime. For example, British dominance in undersea cables led the French, Germans, and Americans to advocate for keeping the lines neutral, even in war. British firms publicly declared their neutrality but in actuality deferred to British political interests, particularly at moments of great tension, and gave up neutrality entirely during periods of war. The power that comes from disrupting or intercepting rival information flows has generally been too alluring for even sincere claims of neutrality to endure.

6. **States often seek their own telecommunications champions once they recognize the vulnerability of relying on a competitor or adversary's firms.** The United States currently lacks a major manufacturer of 5G base stations, which has prompted debates about whether it should invest in its own companies or rely on allied companies. It has also spurred disagreement over to what degree Huawei is itself a de facto state champion. These debates have some precedent. In the early 20th century, many states reliant on others for telecommunications equipment or networks began to build their own systems. For example, Germany pushed two German companies with competing radio efforts — Siemens & Halske and AEG — together to establish a German alternative to British dominance in radio. Many other leading states backed companies that, while ostensibly private, were intertwined with the states that supported them.

7. **The struggle for telecommunications standards can determine which states will wield network power, and it often requires enlisting allies and partners.** States whose technology becomes the dominant standard can wield that leverage over others. The current contest over information communication technology standards is, in this way, similar to the Anglo-German contest over radio networks. Britain, through the Marconi Company which it supported, was so dominant in wireless radio that all other great powers had to pass messages through Britain's wireless network, which refused to engage with any other wireless stations. Germany ultimately found success breaking that dominance at a standard-setting body that prohibited this "non-intercommunication" policy with the help of other powers, including the United States and France — a demonstration of how similar coalitional approaches today could be used by liberal states to set or preserve favorable information and communications technology (ICT) standards if they work together.

8. **States turn to encryption as their communications become easier to intercept, but encryption often has limits due to determined adversaries or user error.** Some argue that anxieties over Huawei's role in networks or over the general vulnerability of devices connected to the internet is ameliorated by modern encryption. These kinds of arguments have a long history. At the dawn of telecommunications a century ago, the possibility that telegraph messages could be read by others who controlled network nodes, or that radio could be intercepted by passive listening equipment, led to major encryption advances that bred occasional overconfidence. Germany's complex rotor cipher machines were believed to be unbreakable, but user error and British industrial-scale efforts allowed Great Britain to compromise German codes. Low-cost updates to German equipment and ciphers could have ended Britain's advantage, but Berlin's overconfidence in its encryption forestalled those alterations, yielding intercepted intelligence that reshaped the course of the war. End-to-end encryption is significantly more advanced than prior efforts at encryption, but history suggests some humility is necessary.

9. **Many states discount the degree to which an adversary may make extraordinary efforts to compromise their networks.** Amid debates over modern telecommunications, it is worth noting that states that prioritized convenience or commerce, and therefore took security shortcuts, have often been unpleasantly surprised by the efforts a determined adversary will make to compromise their networks. In World War I, Germany was surprised by the speed and ruthlessness with which Britain cut all the cables Germany used to access the outside world; similarly, Russian commanders were surprised when their radio indiscipline led to a disastrous defeat at Tannenberg. In World War II, Germany did not expect the British to build a highly-centralized, industrial-scale code-breaking operation that could exploit German communications errors — no matter how trivial or fleeting — to break German codes. And during the Cold War, the Soviets never encrypted an internal underwater telephone line they believed was outside the reach of the United States, but Washington nonetheless found a way to tap it — gaining an invaluable source of intelligence.

10. **Network security is not only about interception, but also about denial.** Some of the debate over Huawei's role in networks emphasizes questions of data security but could benefit from greater consideration of network denial, which has been an important part of great power telecommunications competition. The dawn of telegraphy saw great powers seek to cut cables and deny communications, culminating in Great Britain's unprecedented and well-planned operation to sever all of the cables around the world that could connect Germany to the outside. Sometimes, a state may harm itself in pursuing network denial strategies, but will nonetheless proceed if it believes the harm is greater to its opponent.

THE GREAT POWERS AND TELECOMMUNICATIONS

“Large empires went to great lengths to speed the flow of information,” notes one history of telecommunications. “The Romans built roads, the Persians and Mongols established relays of horses, the British subsidized mail steamers.”[2] But even though states craved information, flows of it remained limited until the dawn of the modern telegraph. The electrification of information flows created modern telecommunications, and with it, familiar patterns of great power rivalry over it.

Those first decades of modern telecommunications, which spanned from 1840 to World War I, share important characteristics with the present moment. That period, like the current post-Cold War era, was one of relative great power peace that made leading states “less sensitive” to questions of politics and security in telecommunications networks.[3] As great powers built out national and international networks in the 19th century, many were initially content to leave industry in charge, ignore the nationality of private companies, and downplay the risks of an adversary’s control over telecommunications networks. The benefits of revolutionary changes in telecommunications — what some at the time called “the annihilation of time and space”[4] — were so obvious and overwhelming that “ownership of the cables was seen as a minor issue.”[5] Telegraphy was about business more than politics in that period, notes one historian in an observation that might just as easily have applied to some of the initial excitement about modern information technology and its latest incarnation: 5G.[6]

The period of relative great power complacency was not to last. States like Peru in 1879 and then the United States in 1898 were some of the first to cut off a rival’s telecommunications networks. As great power tensions heightened, states around the world awakened to find that some — namely Great Britain — had managed the long peace well, and through their private firms, gained a stranglehold on international communications.

As great power tensions heightened, states around the world awakened to find that some — namely Great Britain — had managed the long peace well, and through their private firms, gained a stranglehold on international communications.

Increasingly fearful of dependence on British undersea cable networks, states like France and Germany heavily subsidized the development of their own networks in a development not so dissimilar from China’s own subsidization and protection of its information technology champions like Alibaba, Baidu, Tencent, and Huawei. And as historian Heidi Tworek documents, Britain’s rivals also made large bets on the next generation of telecommunications technology — “wireless telegraphy,” better known as radio — hoping to decrease dependence on British-owned undersea telegraph cables.[7] While the British led in this field, Germany refused to rely on British networks. It built its own network with state-backed champions plowing into less-connected parts of the world — Latin America, Africa, Asia — in what today might mirror the expansion of Chinese technology companies into the developing world and Beijing’s determination to lay the foundations for 5G networks.

Throughout this period, many of the elements of great power telecommunications competition sometimes neglected today were often taken quite seriously by that era’s states. Germany, frustrated with British dominance in radio networks, used a standard-setting body to break British dominance — a tactic that demonstrates that those bodies were no less important in that era than they are now. And as telecommunications went wireless and became even easier to intercept, great powers put their faith in encryption — sometimes foregoing disciplined operation of their networks under the assumption that "ciphers" — detailed steps to encrypt or decrypt messages — would solve the problem, a belief that almost always proved erroneous due to user error. That view has striking parallels to modern assumptions about the general insecurity of telecommunications networks, and the belief articulated by some in debates over Huawei that encryption would largely neutralize the risk of China's access to one's telecommunications network.

When the great power peace ended and war erupted, the political importance of telecommunications — not always clear in peacetime — was suddenly evident. German success in intercepting Russian transmissions in World War I produced a victory so thorough in the Battle of Tannenberg that it changed the course of the war and helped precipitate Russia's exit from the conflict. British dominance of undersea cables in World War I was so complete that it cut off Germany from the global telecommunication system, routed German cable traffic through its own networks, and ultimately uncovered the Zimmerman telegram, which helped bring the United States into the conflict. In World War II, Britain scored another intelligence success by breaking German encryption that had been presumed unbreakable, leading to unparalleled intelligence that Britain's official histories argue shortened the war in Europe by years. These cases demonstrate that telecommunications security is not simply a matter of battlefield tactics but of political competition, one that can dictate the fates of great powers and the shape of world history.

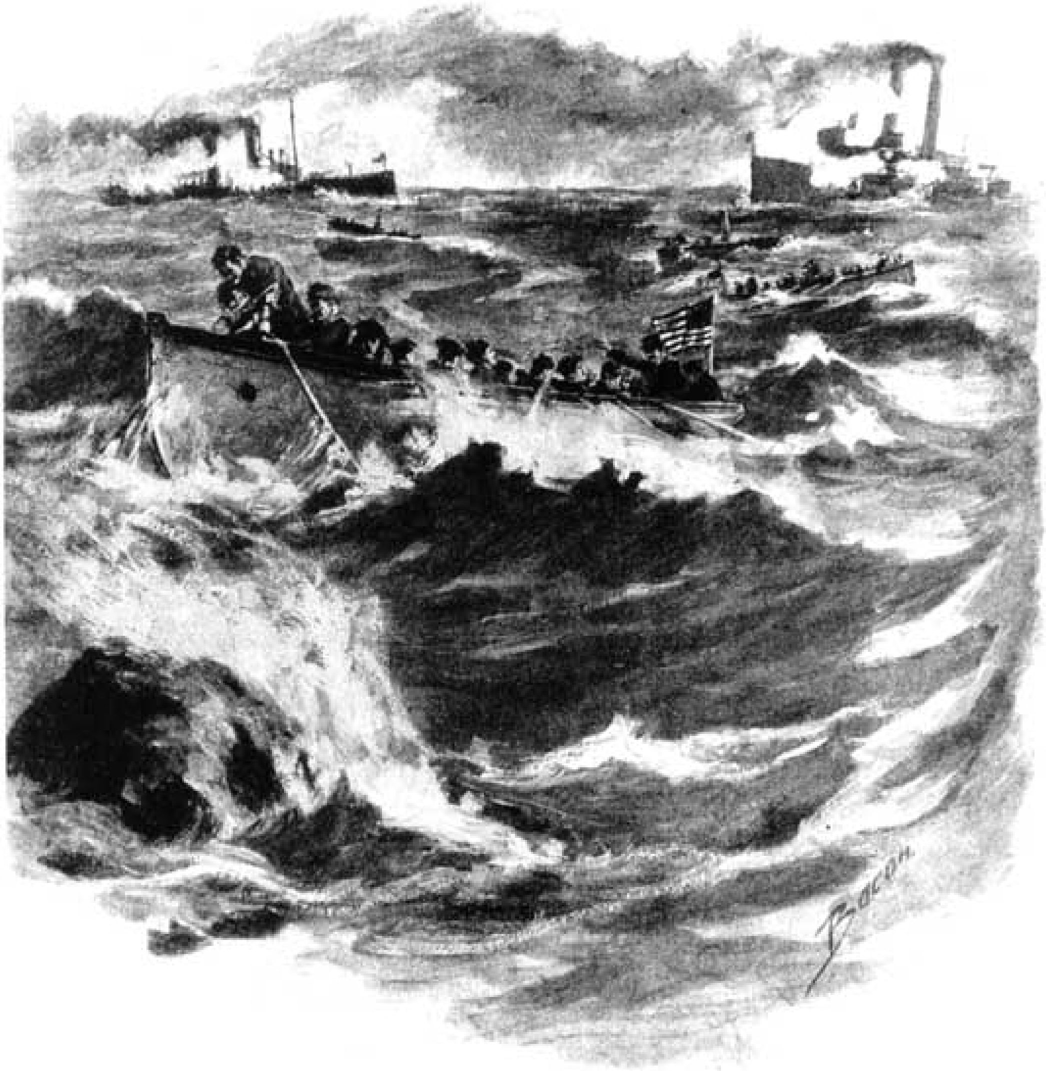
Telecommunications, as this brief series of cases shows, has always been political.

As the world moved into a U.S.-Soviet Cold War, British advantages were dislodged not only by American power but by shifts in technology that made older networks less relevant, demonstrating the importance for great powers to remain at the forefront of technology. In that new era, telecommunications competition continued along familiar lines. For example, the United States pioneered new ways to tap submarine cables that were buried so deep and considered so secure that messages across them were often left unencrypted. Competition moved into other domains, too — such as satellites and internet infrastructure — though much of this history is still being written and, in most cases, remains classified.

Telecommunications, as this brief series of cases shows, has always been political. The exploitation of these technologies and capabilities has generally evolved alongside their development. As soon as new methods of communication arrived, great powers generally looked for ways to intercept or interrupt them. "Electrical communications has often been described as one of the great achievements of mankind," notes one historian of telecommunications, "but when we look at it from a security point of view, we see an entirely different picture, for security is not a technical but a social and political characteristic." And "since politics have not improved," he notes, "telecommunications has a dark side."[8]

We now turn to a summary of the key themes in almost two centuries of telecommunications competition.

1. THE SPANISH-AMERICAN WAR: THE LIMITS OF CABLE NEUTRALITY



A depiction of the U.S. cable-cutting expedition at Cienfuegos published in 1907. The operation demonstrated that undersea telegraph cables would not be treated as neutral during armed conflict, even by a great power that had once advocated cable neutrality. Source: Naval Historical Center Online Library[9]

As submarine cables began to crisscross the world in the 19th century, several leading powers — including France, Germany, and the United States — called for them to be kept isolated from international politics. In 1858, in one of the first ever trans-Atlantic cables ever sent, U.S. President James Buchanan urged Queen Victoria to ensure that the world's new telegraph lines be kept "forever neutral… even in the midst of hostilities."[10]

Once hostilities broke out, however, high-minded principles of neutrality were abandoned. Two decades after Buchanan's message, Peru cut Chilean cable lines running into disputed territory.[11] That dispute received little attention, but when the United States — an erstwhile champion of cable neutrality — cut cables in both the Atlantic and the Pacific in the Spanish-American War, the world took notice.

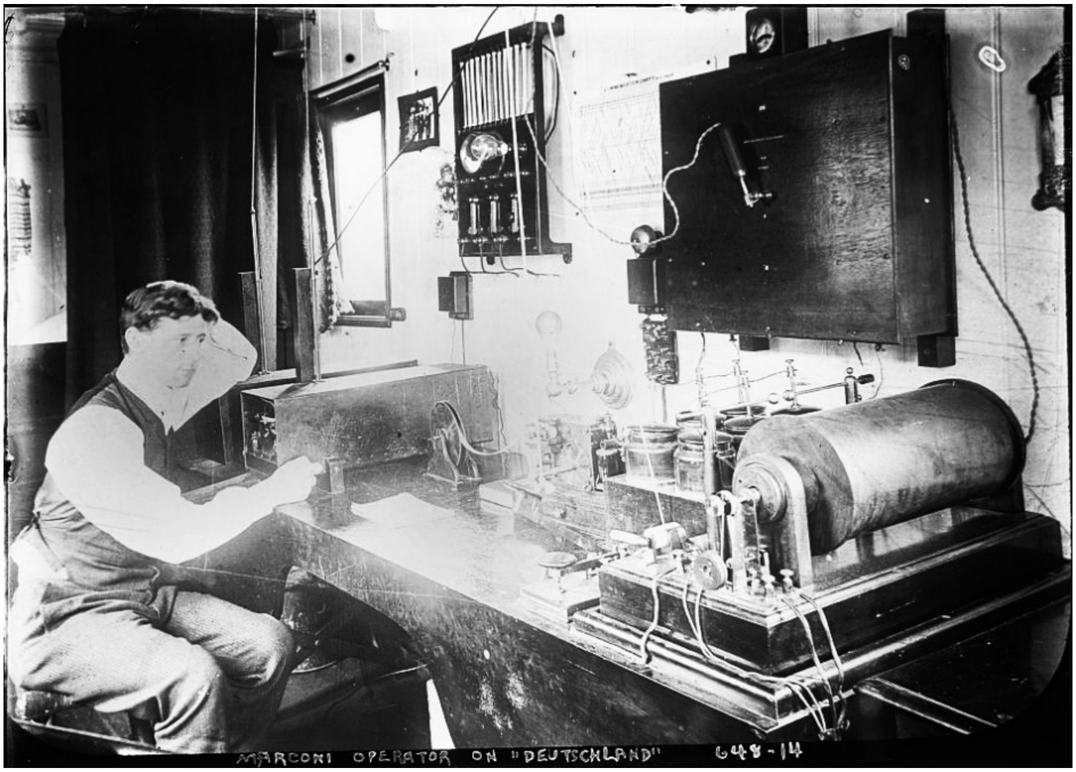
American cable cutting was planned in advance of the conflict. In the Atlantic theater, the United States had hoped to cut off Spain from its forces in Cuba. “The isolation of Havana was, of course, of prime importance,” noted one American magazine account at the time, and that required the United States to “shut off Havana from all telegraphic communication with the outside world.”[12] The United States started by cutting off Spanish traffic that traversed American territory in Florida. Then, it dispatched a small American outfit to destroy a key telecommunications node in Cienfuegos, cutting off the city of Havana and much of western Cuba from Spain. Afterwards, the United States attacked various cables in eastern Cuba as well as Caribbean cables that connected Puerto Rico to Spain.[13] Together, cable cutting significantly degraded Spain’s ability to direct and command forces in Cuba.[14]

When the United States — an erstwhile champion of cable neutrality — cut cables in both the Atlantic and the Pacific in the Spanish-American War, the world took notice.

In the Pacific, the United States cut the only submarine cable between Manila and Hong Kong, effectively severing the Philippines from Spain.[15] The decision harmed U.S. communications, too, but it was presumed to impose an even greater cost on the Spanish, and the United States was able to compensate by dispatching one vessel regularly to Hong Kong to wire dispatches back to Washington.[16] U.S. forces also cut undersea cables within the Philippines, further degrading Spain’s ability to command its forces.

The Spanish-American War was perhaps the first global conflict spanning multiple theaters in which electrical telecommunications mattered. It also marked the first time that one great power sought to deny another access to undersea cables. Before the conflict, telegraphy was still seen as a primarily commercial realm, and many had hoped cables would remain walled off from political and military competition. The conflict proved the limits of such perspectives, and indicated that control over telecommunications infrastructure and the ability to deny those advantages to geopolitical rivals has always been of critical political significance.

2. THE ANGLO-GERMAN RIVALRY: BUILDING NETWORKS AND SETTING STANDARDS



Marconi Company radio operator in the "Marconi Room" of the German ocean liner SS Deutschland. The Marconi Company's influence was so great that their employees operated in German radio rooms even though Germany was concerned about the risks of interception and denial. Source: Library of Congress, George Grantham Bain Collection[17]

Technological standard-setting, and its attendant network effects, is a longstanding and subtle arena of great power competition. States whose technology becomes the dominant standard can wield that leverage over others—a point not lost on rising powers, who often work to reduce their vulnerability by creating parallel systems. Indeed, the present Sino-American contest over ICT mirrors a century-old contest between Germany and Great Britain for dominance in that era's ICT infrastructure, with uncanny parallels and key lessons for the present.

States whose technology becomes the dominant standard can wield that leverage over others — a point not lost on rising powers, who often work to reduce their vulnerability by creating parallel systems.

In the late 19th century, Italian engineer Guglielmo Marconi, supported by the British Royal Navy, created wireless telegraphy.[18] The invention was revolutionary. While great powers cut each other's cables in the past, and while ship-to-ship and ship-to-shore communications had previously been difficult, Marconi's system solved those problems and was less prone to interference.[19] Marconi ultimately partnered with Great Britain, affording the country a monopoly over radio transmissions. When combined with

Britain's 60% share of the world's undersea cable network, Britain dominated international transmissions. The British advantage was unsettling to Germany, but competition over wireless technologies also "presented an opportunity for Germany to exert control over a new international infrastructure" and to "circumvent British cables;" great power primacy was tied up in the outcome.[20]

Feeling vulnerable, Kaiser Wilhelm II authorized direct state support for German scientists and engineers as they successfully copied Marconi's designs, patented them within Germany, and built their own radio networks financed by contracts with the German military.[21] Even so, Marconi's superior longer-range radio and first-mover advantage established his British-backed company as the global standard, and Marconi leveraged these network effects to pursue a policy of "non-intercommunication" with non-Marconi radio operators. German businesses and ocean liners did not want to be cut off from global communication, so they preferred the British-backed system to German ones.

Kaiser Wilhelm II intensified German industrial policy to contest the British standard. He swiftly decreed that two large German electrical companies with competing radio efforts, Siemens & Halske and AEG, join together to establish the definitive German alternative, Telefunken. "The [domestic] rivalry in the field of wireless telegraphy weakens the competitiveness of Germany," the kaiser explained, "and gives the Marconi Company the opportunity to reach a worldwide monopoly" that was "not in Germany's interest."[22] Under Kaiser Wilhelm II, Germany pursued protectionism by banning the Marconi systems in some cases. It pursued emerging markets by selling its technology to South America and Africa to set the standard in those regions and secure revenue.

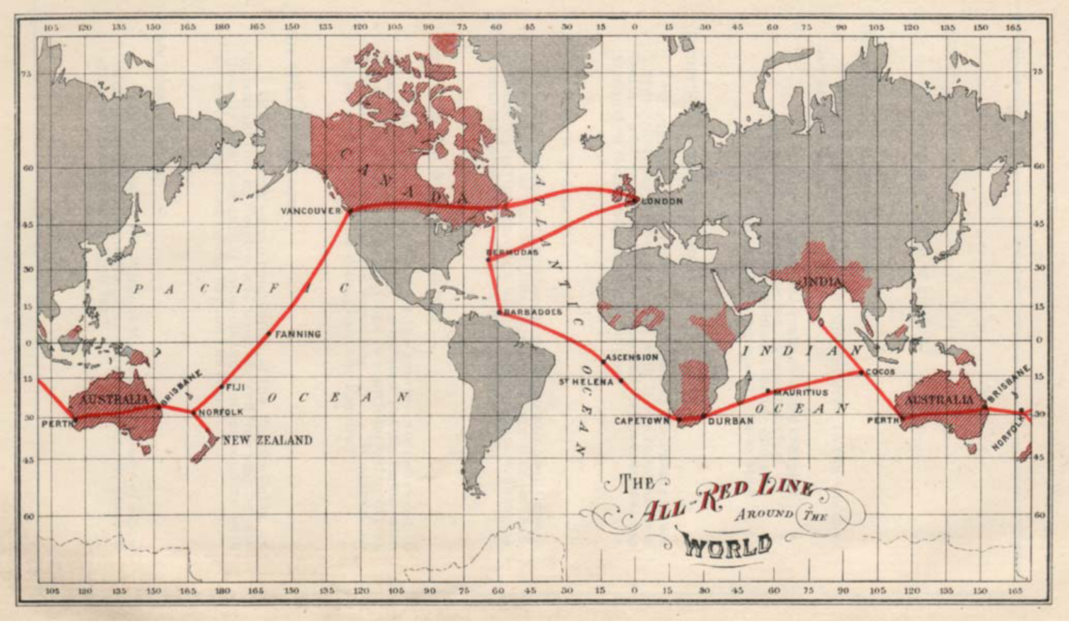
When those efforts proved inadequate, Germany found success in multilateral standard-setting bodies. In 1906, Germany organized the great powers together in the first International Radiotelegraph Convention, a conference on radio standards. There, the members jointly prohibited Marconi's "non-intercommunication" policy, breaking the British monopoly and establishing an effective Anglo-German duopoly.[23]

The Anglo-German competition reveals that standard-setting bodies have enormous strategic implications. China today uses many of the techniques that Germany used a century ago — state-led industrial policy, state protection, generous state contracts, civil-military integration, bans on rival products, forced mergers, the pursuit of emerging markets, and even international treaties to set its standards — all of which has helped Chinese technology companies like Alibaba and Tencent, the owners of WeChat and AliPay, to become local champions. These companies have since expanded overseas, often targeting not the U.S. market but — like Germany's Telefunken before them — emerging markets with lower profits and reduced competition.[24]

China is also contesting standards in the hard infrastructure of internet connectivity. Its government is investing billions so Chinese chipmakers can beat American rivals in the race for 5G mobile internet standards. Similarly, Chinese firms like Huawei and ZTE receive government loans to build the hard infrastructure of internet connectivity throughout the developing world. As the British example demonstrates, these efforts not only make Chinese technology the standard, they also offer opportunities for surveillance. Meanwhile, the Belt and Road Initiative raises the possibility that standards for "smart infrastructure" across Asia, especially the relevant sensors and software, may be set by China and may deny other companies interoperability, thereby shutting them out of autonomous vehicles and other industries.

The Anglo-German rivalry in telegraphy shows that Washington needs to take China's state-directed challenge in standards seriously. It also offers a way forward. In much the same way Germany used international conferences to break the British monopoly on telegraphy, the United States could set or preserve favorable ICT standards through multilateral agreements. Doing so may keep China from unilateral standard-setting through its free trade agreements, state champions, or infrastructure projects.

3. BRITAIN IN WORLD WAR I: DEPLOYING INFORMATION HEGEMONY



The "All Red Line," a costly network of British undersea cable lines built with enormous redundancies and arranged so that no part passed through a rival's territory. Germany's inadequate investment in its own resilient global telecommunications network enabled Britain to cut it off from global communications while Britain remained generally unaffected. Source: George Johnson, ed., The All Red Line: The Annals and Aims of the Pacific Cable Project / Internet Archive[25]

Germany's efforts to break British dominance in telecommunications in the early 20th century were not born of paranoia. Once World War I broke out, Britain successfully wielded its considerable influence in telecommunications networks to shape the course of the war. It cut German cables, monitored German transmissions, and forced German traffic onto British-controlled networks — uncovering the Zimmerman telegram, which helped bring America into the war.[26]

Germany's efforts to break British dominance in telecommunications in the early 20th century were not born of paranoia.

Great Britain was not the first great power to cut or manipulate telecommunications networks: Peru had cut a Chile-Bolivia link, the United States had cut Spanish cables, and Britain had cut off the Boers from their European supporters in one crisis and manipulated cable traffic to France in another.[27] But these efforts were taken to the extreme in World War I.

Great Britain was the first to cut off an entire country from mainstream global telecommunications networks, deploying on the first day of the war a plan carefully put together in peacetime.[28] Within a year, Great Britain destroyed German cables worldwide: in the English Channel, the North Sea, the North Atlantic, South America, much of Africa, the Far East, and even in neutral countries that hosted German infrastructure.[29]

To compensate, Germany tried to expand the radio network that Telefunken constructed a decade earlier in Latin America and the "Global South" so that it would cover the world. In an effort with modern parallels in China's Digital Silk Road, Berlin offered loans and investment to governments interested in the "developmental benefits of radio" so they would host German communications nodes. In response, Great Britain persuaded or induced most of these countries to forego support for German radio nodes or actively sabotaged them.[30]

Left without networks of its own, Berlin had no choice but to rely on Britain's network during the war. At the outset, the British began quietly monitoring all traffic that passed through their cables and used the advantage to wage information warfare against Germany, selectively leaking embarrassing German traffic to damage its relations with neutral countries. When Germany sent a telegram proposing a military alliance with Mexico against the United States — the infamous Zimmerman telegram — the message traversed a British network and was intercepted and decrypted by Great Britain, who then shared it with the United States government, which in turn shared it with the American public.[31] That incident helped bring the United States into the war, shaping world history and eventually sealing Germany's defeat.

British information warfare against Germany reveals the dangers of affording a rival power the ability to monitor one's traffic or shut off one's telecommunications access. It also reveals that the networks great powers take for granted in peacetime are often denied in wartime, and that the struggle for communication nodes will inevitably involve third parties and neutral countries.

4. GERMAN VICTORY AT TANNENBERG: THE DANGERS OF INTERCEPTION

A German wireless field telegraph station during World War I. Russia's inability to adequately encrypt its communications at its field stations led to a disastrous defeat that reshaped the course of the war. Source: C. O. Nordensvan and Valdemar Langlet, Det stora världskriget *[The Great World War] / Wikimedia Commons*[32]

Germany was not entirely without its own capabilities in information warfare. It cut Russian overland and undersea cables that connected it with its Western allies, as well as several transatlantic cables upon which the British relied, pioneering the use of submarines for these tasks.[33] Given the redundancy of British networks, these efforts were ultimately less debilitating than the Germans had hoped. What proved far more consequential was Germany's use of radio intelligence against Russia during the Battle of Tannenberg in August 1914, the first month of the war, precipitating a disastrous defeat for the Russians. One German intelligence officer at the time called the incident "the first in the history of man in which the interception of enemy radio traffic played a decisive role."[34]

The battle took place amid Russian gains on the Eastern front. As Russia proceeded deeper into East Prussia, its military encountered a significant communications challenge that set the stage for a disastrous defeat. The retreating Germans had cut their own telegraph lines, and the advancing Russians lacked enough trained personnel to set up wired communications across their sprawling formation. Radio transmission provided an alternative, but while the Russians had adopted new radio technologies for their military command and control, they had not adequately secured them. Different groups had been assigned different ciphers; most had little training with encoding and decoding signals; some codes were known to have been broken by the British; and code books were limited or unintelligible to many of the illiterate conscripts.[35] The result was that Russian commanders felt they had to take the risk of using uncoded radio messages and hope the Germans were not monitoring them carefully.

The Germans, however, were monitoring the signals closely. Having observed Russian radio indiscipline in war against the Japanese, they knew that Russian uncoded transmissions were not part of a deception campaign. They then used their knowledge of real-time Russian communications to lift the "fog of war" and decisively defeat the superior force. Russia lost an entire army, with over 100,000 casualties and 92,000 taken prisoner compared to only 13,000 German casualties.

5. BRITAIN IN WORLD WAR II: THE LIMITS OF ENCRYPTION

Mechanical rotors of the Lorenz enciphering machine considered effectively unbreakable during World War II. British efforts to break the cipher gave officials access to high-level German communications. Source: Matt Crypto / Wikimedia Commons[36]

The inventions of wireless telegraphy and radio brought greater convenience, relative to physical cables, but carried greater risk of interception. In World Wars I and II, the great powers existed in a world where radio communications were assumed to be accessible to others. And in such a world — not so dissimilar from present assumptions about the vulnerability of modern computer and telecommunication systems — encryption was deemed critical to security. The result, as one American military historian put it, was a "struggle between the cryptographer and the cryptanalyst."[37] When great powers were on the wrong side of that struggle, the results could be catastrophic.

In World Wars I and II, the great powers existed in a world where radio communications were assumed to be accessible to others... Encryption was deemed critical to security.

To prevent such an outcome, organizations would use ciphers to reduce the risk that interception would compromise security. They also exercised "radio discipline" to prevent adversaries from gleaning insights about usage patterns through radio traffic analysis.

Most great powers invested in a truly industrial effort to study adversary traffic and, if possible, to break adversary ciphers. Great Britain was far more centralized in its analysis of adversary ciphers than Germany, which had those functions spread among several agencies. And just as British successes in signals intelligence and cryptoanalysis had shaped the course of World War I, so too did they shape the course of World War II when the British operation at Bletchley Park broke Germany's Enigma and Lorenz ciphers.

The Enigma and Lorenz ciphering systems used extraordinarily complex rotor machines to encrypt messages that Germany believed "would remain invulnerable."[38] Each keystroke would replace a character with another character based on unique settings for the machine, and those settings — which, for the Lorenz system, exceeded the total number of atoms in the universe — needed to be shared by the sender and receiver to read the message.[39] Enigma was used by the military, the Gestapo, and diplomats; Lorenz, which was even more complex, was used by Adolf Hitler and senior Nazi and military officials to communicate with each other.

British success in breaking Enigma and Lorenz was a product of several developments. First, it was a product of allied intelligence cooperation with Poland, which had exploited some German errors to break some simpler Enigma machines.[40] As one British cryptanalyst of the time put it, their effort "would never have got off the ground" without Polish contributions.[41]

Second, it was a product of German overconfidence, with Germany never suspecting the ciphers were broken and therefore forgoing fairly easy modifications that would have forced Britain to begin all over.[42] Even so, German faith in the invulnerability of its machines "was almost right," recounted one senior Bletchley Park official.[43]

Finally, it was the product of a single but major lapse in German "radio discipline" that created an opening to reverse engineer German ciphering systems despite never having seen one in person.[44] Even the most sophisticated systems were vulnerable to user error, and a vigilant adversary could exploit it.

By breaking Enigma and Lorenz, Great Britain had access to some of Germany's most sensitive communications. Winston Churchill reportedly credited the intelligence with having been a key reason Great Britain won the war, and Dwight D. Eisenhower reportedly called it "decisive."[45] The official historian of British intelligence, Sir Francis Harry Hinsely, argues that these successes "shortened the war by not less than two years and probably by four years," undermining Field Marshall Erwin Rommel in Africa, sharply reversing allied shipping losses to German U-boats, and enabling the Normandy landings.[46] They also allowed Britain to identify virtually all German spies entering the country and often turn them or use them to pass back faulty intelligence, with the head of the program noting that British intelligence "actively ran and controlled the German espionage system in this country."[47] Few countries have ever had such intimate knowledge of another during wartime.

Taken together, the successes of Britain's efforts against Germany, Poland's peacetime monitoring of German communications, and its decision to share its breakthrough with Great Britain, have lessons applicable to today when great powers conduct cyber reconnaissance against each other. More broadly, those who suggest encryption mitigates the problems of an adversary's access to one's telecommunications network may be making a mistake not dissimilar from that Germany itself once made: excessive faith in technology and limited attention to the ever-present possibility of human error.

6. OPERATION IVY BELLS: THE DEPTHS OF INFORMATION PURSUIT

The USS Halibut, which was reportedly involved in an effort to tap an undersea Soviet telephone line. Source: U.S. Navy / Wikimedia Commons[48]

The Soviet Union was much more careful with its encryption than the Nazis had been, relying on their own version of Enigma — known as Fialka — that was substantially more complex.[49] For that reason, the vast troves of strategic-level intelligence produced in World War II after German ciphers were broken had no publicly known analogue in the Cold War. Given these challenges, other methods of penetrating adversary telecommunications were pioneered. One of the most audacious of these efforts took place with respect to undersea cables.

The dawn of undersea cables in the 19th century had eventually led to efforts to cut and occasionally tap them, often in shallower waters or on land where such tasks were easier to conduct. In contrast, performing these operations in deep waters controlled by an adversary was thought virtually impossible, particularly if it was to be done covertly. Beginning in the 20th century, the British and then successive great powers had come to a determination about undersea cable security: if the landing sites were secured, and the cables did not traverse neutral or unfriendly countries, then they would generally be secure from interception and often safe from being cut, particularly in peacetime.[50]

During the Cold War, however, that calculus changed. The advent of nuclear submarines opened up the possibility of tapping undersea cables in deeper water. But the task of dispatching divers to access cables on the deep seafloor was thought to be more akin to space exploration than the familiar attempts at cable manipulation attempted in previous eras. Creating a tap that could be installed in such conditions was technically challenging, too.

When the United States suspected that a Soviet undersea cable might run from the naval headquarters in Vladivostok to a submarine base on the Kamchatka peninsula, it sought to overcome these obstacles, demonstrating the value of signals intelligence.[51] Tapping that five-inch bundle of wires, it was believed, would provide critical information on Soviet nuclear forces.[52] While the Soviets encrypted all traffic sent through the air, the United States expected that the Soviets would presume traffic through the protected undersea cable was virtually impossible to access, and therefore would not encrypt it. Moreover, “Soviet admirals and generals would be far too imperious and impatient to suffer an ocean of cryptographers already overwhelmed by the sheer bulk of their work,” and would insist on unsecured voice communications.[53] A tap then would provide a rare trove of intelligence, and the U.S. Navy launched Operation Ivy Bells to establish it.

Much about the tap and the intelligence garnered from it remains classified, but open sources provide some details on the unique and innovative operation. The United States dispatched a nuclear submarine, the USS *Halibut,* to quietly sneak past the Soviet navy and find the submarine cable in an area spanning 600,000 square miles.[54] Innovative technology was created to ensure that divers could work under great pressures and in extremely cold temperatures for stretches of several hours. Similarly, new methods for installing a tap in this challenging environment were devised.[55] All of this had to be done without any Soviet detection or suspicion. If the ship were detected, the Soviets might board or destroy it.

The operation ultimately proved successful, and throughout the 1970s, the U.S. Navy tapped and recorded unsecured messages across the cable. Every few months, American submarines would quietly slip into Soviet waters, evade attack submarines, deploy divers to the tapped cable lines, and retrieve tapes of Soviet communications — yielding an extremely valuable and rare sliver of intelligence. While the United States had expanded a “network of spy satellites, planes, listening stations, and subs” to gather signals intelligence, it “could not penetrate a hardwired phone line” within an adversary’s territory. This effort illustrated the evolutionary shift in telecommunications, namely that data and signals transmitted through any medium and by any means could be accessed by a determined actor with the right tools. While this tap was ultimately compromised by a leak, the resulting telecommunications intercepts provided invaluable military and political intelligence to the United States and its allies.[56]

Every few months, American submarines would quietly slip into Soviet waters, evade attack submarines, deploy divers to the tapped cable lines, and retrieve tapes of Soviet communications — yielding an extremely valuable and rare sliver of intelligence.

MODERN TELECOMMUNICATIONS COMPETITION IN HISTORICAL PERSPECTIVE

By the end of the Cold War, the United States had clearly replaced Great Britain as the information hegemon. The United States maintained a nodal position in the global internet, robust space capabilities, dominance in most internet technology, and — according to public disclosures — sophisticated abilities to intercept or possibly deny adversary communications.

These American advantages are now being tested, like Great Britain's over a century ago. Russia, and especially China, now challenge U.S. dominance. While the United States enjoys a nodal position in many data flows, other powers are increasingly seeking to reduce their dependence on U.S. networks. At the same time, the nodal American position is less necessary for interception than Great Britain's was a century ago. The internet makes intrusion possible without control over physical infrastructure. Smartphones and computer networks can be hacked, and whether one's sensitive communications are compromised by the physical taps of an earlier era or by the virtual intrusions of the modern one, the end result is the same. Connection in this way likely creates greater vulnerability now than it did in the era of the telegraph or wireless radio.

> **Smartphones and computer networks can be hacked, and whether one's sensitive communications are compromised by the physical taps of an earlier era or by the virtual intrusions of the modern one, the end result is the same.**

Russia has been a leading state in exploiting that vulnerability. In 2007, Russia launched a wave of cyberattacks against Estonian institutions, mostly distributed denial of service attacks.[57] In 2008, it launched cyberattacks in the Russo-Georgian War. These involved not only directed denial of service attacks, but also efforts to redirect government websites, take over Georgian government servers, and reroute Georgian internet traffic through Russian-controlled servers — with some of the attacks staged in advance of the conflict to coincide with Russian military action.[58] In 2014, when Russia invaded Crimea, it combined cyberattacks with physical control of telecommunications networks. Russian soldiers seized Ukrainian telecommunications facilities, using them to cut off communication in Crimea and even to carry out cyberattacks and disruption in other parts of Ukraine.[59] In 2015, Russia began a wave of cyberattacks on Ukrainian infrastructure, knocking out power for hundreds of thousands of Ukrainians in two major instances. Over the next several years, it proceeded to launch a wave of unprecedented attacks across Ukraine spanning "media, finance, transportation, military, politics, and energy" — virtually every segment of Ukrainian society — in what some believed was partially an effort at training for a similar campaign against the United States.[60] At the same time, it continued a range of attacks across the Baltics and famously sought to shape the U.S. election in 2016 and 2020 with disinformation campaigns, as well as other countries.[61] In 2021, the U.S. government formally accused Russia of the hack of IT company SolarWinds, a sophisticated attack which compromised much of the federal government and several major U.S. companies.[62]

China is the other major power making significant investments in telecom competition, though unlike Russia, China's efforts not only seek to exploit existing internet infrastructure but also to build networks and infrastructure it can influence and even control. Like Russia, China has been adept at exploiting existing internet vulnerabilities. In the early 2000s, it launched a wave of attacks on U.S. Department of Defense networks in what the department termed Operation Titan Rain.[63] Governments around the world — the United States, the United Kingdom, France, Germany, Canada, Australia, Japan, South Korea, Taiwan, India, and over a dozen others — have complained about Chinese intrusion into their government networks. Some of the largest cyberattacks of the last decade were confirmed by U.S. Attorney General William Barr to have been perpetrated by Chinese agents, including thefts of records from the U.S. Office of Personnel Management (records for 21 million people), Marriott hotels (for 400 million), Anthem health insurance (for 80 million), and Equifax (for 147 million), among others.[64]

At the same time, China is also laying the foundation for future internet infrastructure and, in light of its previous efforts, it is unlikely that this effort is commercial now or will remain purely commercial in the period ahead. China's investments are most pronounced in the 5G networks expected to form the foundation for a smarter, connected economy linking countless devices and sensors together. Eager to build these networks worldwide, China has subsidized its 5G champions and projects around the world as part of a Digital Silk Road initiative. With competitive pricing, companies like Huawei were able to outcompete other major 5G vendors and command a significant global market share, making China a leader in building these networks. And outside of 5G, China's government has subsidized efforts to build internet or communications infrastructure on virtually every continent. These efforts are all supplemented by a campaign to shape global standards, a key policy priority for China enshrined in high-level planning documents that — as in the Anglo-German rivalry over radio a century ago — could shape the future of telecommunications in ways that advantage China. To that end, China recently unveiled a new data security initiative.[65]

From that broader historical perspective, the evidence may lead many observers to conclude prudence is warranted about the role of Huawei in telecommunications networks — even if the company's motives are indeed purely commercial, its promises of "no backdoors and no spying" are credible, and Beijing is sincere in its commitment to honor those pledges.

Some fear that China's activities leave open the possibility that Beijing will have de facto control over these networks, whether to intercept traffic or deny access. Little public information is available about China's efforts to acquire that control, but the U.S. government revealed in February 2020 that Huawei had backdoors in its network equipment, did not reveal them to the relevant companies with which it contracted, and that the backdoors went beyond those sometimes requested by host governments as part of lawful intercepts.[66] Moreover, public reporting has revealed that Huawei assisted governments like Uganda and Zambia with compromising the identities of dissidents.[67] Even beyond the Huawei case, a cybersecurity firm recently discovered backdoors in mandatory tax software the Chinese government requires foreign companies to install.[68] Regardless of whether these cases suggest that Huawei has itself exploited its position in these networks, the company's behavior and China's track record with cyberattacks and espionage, are reasons for concern.

The other major reason for concern comes from history and the behavior of even liberal great powers more thoroughly constrained by the rule of law. Indeed, the preceding historical cases strongly suggest that the kind of power and influence a company like Huawei will wield is likely to be exploited by the Chinese government, just as other great powers have often exploited the position of their companies or capabilities in telecommunications.

From that broader historical perspective, the evidence may lead many observers to conclude prudence is warranted about the role of Huawei in telecommunications networks — even if the company's motives are indeed purely commercial, its promises of "no backdoors and no spying" are credible, and Beijing is sincere in its commitment to honor those pledges.

More broadly, as this report shows, many of the features of great power telecommunications competition that are considered novel today have roots in the past. Across history, several themes have recurred:

- *Power:* Control over telecommunications networks has been a form of political power since its inception over 150 years ago. Great Britain exploited its role in telecommunications and radio, the United States likely has done so in the modern internet era, and there is reason to be concerned that China may attempt to do so today.

- *Complacency*: Long periods of peace and prosperity have led to complacency about telecommunications risks. In the 19th century, great powers were content to rely on foreign firms and foreign-operated networks, just as states today have been willing to accept Chinese telecommunications equipment and operation. But eventually, reliance on potential competitors or adversaries proved disastrous for countries like Germany and reshaped world politics.

- *Exploitation:* New telecommunications technology has always led to new efforts to intercept, deny, or exploit it. Despite hopes that encryption may complicate China's efforts to intercept modern communications, past periods of great hope in encryption were dashed by user error and the determined efforts of rival states to break them, as Germany discovered when Great Britain broke its supposedly "unbreakable" ciphers. Humility should accompany each wave of supposedly secure technologies.

- *Champions:* States often seek their own telecommunications champions, particularly as great power tensions rise. China's government is proud of Huawei's accomplishments, and champions it around the world — even threatening states that refuse its technology. It would be unusual for a company so close to its home government to be immune from state pressure when so many other telecommunications champions across history have not been.

- *Standards*: Telecommunications standards can determine who wields network power, with Germany using a standard-setting body to break Great Britain's dominance in wireless radio. Today, that competition is underway in bodies like the International Telecommunications Union, and Huawei's role in it suggests the need to consider whether its standards will allow China to reshape telecommunications.

- *Denial:* Network security is not only about interception and data security, but also about denial of the entire network's operation or access to outside networks. Great

Britain cut off Germany from the world's telegraph networks, and Huawei's role in networks might empower it to shut down networks in countries where it is operating equipment even if it is unable to easily access data.

- *Determination:* Many states discount the degree to which an adversary may make extraordinary efforts to compromise their networks, and are later dealt an unpleasant surprise when it does. Britain's ability to break German ciphers in World War II through industrial-scale efforts and the American ability to tap supposedly-untappable internal Soviet submarine cables demonstrates the depths to which great powers will go to access critical signals intelligence. China, too, is likely to undertake such maximum efforts, and even if Huawei will find it difficult to weaponize its position in modern networks, underestimating the resourcefulness and drive of a determined competitor like China is a recurring motif in telecommunications competition.

As this report demonstrates, many of the features of the great power game over telecommunications remain the same, even as the players may be different.

ENDNOTES

[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/.

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

[3] Ibid., this observation is Headrick’s.

[4] Ibid.

[5] Ibid.

[6] Ibid., this observation is Headrick’s.

[7] Heidi Tworek, *News from Germany: The Competition to Control World Communications, 1900-1945* (New York: Harvard Historical Studies, 2019).

[8] Heidi Tworek, *News from Germany: The Competition to Control World Communications, 1900-1945* (New York: Harvard Historical Studies, 2019).

[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.

[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.

[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, November 6, 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 Though as Heidi Tworek notes, his own role has often been inflated in the development of this technology. 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/.

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 (January 9, 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 For example, Telefunken was active even in areas Germany did not have a major colonial presence, like Latin America.

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, December 15, 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, 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).

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 1x10170 possible settings.

40 "Bletchley Park Remembers Polish Code Breakers," BBC News, July 14, 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 See, for example, 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*, April 27, 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*, April 27, 2019, https://foreignpolicy.com/2019/04/27/the-soviets-unbreakable-code-fialka-encryption-espionage-russia-kgb-spy/.

50 Daniel R. 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.

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*, March 30, 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, 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/.

[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.

[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; Sergey Sukhankin, “Russian Electronic Warfare in Ukraine: Between Real and Imaginable,” Jamestown Foundation, May 24, 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/; “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,” U.S. Department of Justice, October 19, 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/.

[62] Maggie Miller, “US intel agencies blame Russia for massive SolarWinds hack,” *The Hill*, January 5, 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*, February 11, 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*, September 8, 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.

[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.

[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.

ABOUT THE AUTHORS

Rush Doshi was the director of the Brookings China Strategy Initiative and a fellow in Brookings Foreign Policy. He was also a fellow at Yale Law School's Paul Tsai China Center and part of the inaugural class of Wilson China fellows. His research focused on Chinese grand strategy as well as Indo-Pacific security issues. Doshi is the author of *The Long Game: China's Grand Strategy to Displace American Orde*r, forthcoming from Oxford University Press. He is currently serving in the Biden administration.

Kevin McGuiness recently worked with Brookings as an extern from the Department of Defense Skillbridge Program, where he contributed to various projects within the Center for East Asia Policy Studies. He is an Air Force veteran and recently finished his tour of duty as faculty at the United States Air Force Academy, directing courses in international relations and Asian politics. He also recently worked as a research assistant with the Institute for National Strategic Studies' Center for the Study of Chinese Military Affairs, where he focused on PLA modernization and security in the Indo-Pacific.

ACKNOWLEDGEMENTS

The authors wish to thank former interns Isabella Lu, Zijin Zhou, and Gaoqi Zhang for their research assistance on this project, several anonymous reviewers, Claire Harrison and Ted Reinert for editing the report, and Chris Krupinski and Rachel Slattery for layout and web design. Brookings is grateful to the U.S. Department of State and the Institute for War and Peace Reporting for funding this research.

This report was completed before Rush Doshi's government service, involves only open sources, and does not necessarily reflect the official policy or position of any agency of the U.S. government.

The Brookings Institution is a nonprofit organization devoted to independent research and policy solutions. Its mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations for policymakers and the public. The conclusions and recommendations of any Brookings publication are solely those of its author(s), and do not reflect the views of the Institution, its management, or its other scholars.

BROOKINGS

The Brookings Institution
1775 Massachusetts Ave., NW
Washington, D.C. 20036
brookings.edu