Digital Chokepoints

Michael Porcellacchia, Christoph Trebesch, Benjamin Wache*

March 2026

Abstract

Submarine telecom cables are chokepoints of the global economy. They carry over 95% of intercontinental data but are highly vulnerable to sabotage, espionage, and sanctions. This paper presents the first systematic effort to map global telecommunications networks over 150 years and to quantify dependence, vulnerability, and hegemonic dominance within this network. We produce the *CableHist* dataset, covering all international undersea telecommunication cables (telegraph, telephone, and internet) from 1850 to 2025, as well as all satellites in orbit. Using a network traffic model, we estimate countries' dependence on foreign-controlled cables and their exposure to disruption. We show that, both in history and today, hegemonic powers dominate the global cable network, and that they have repeatedly weaponized this control. We further show that geopolitical tensions, particularly with the hegemon, induce decoupling, meaning strategic but economically redundant cable investments aimed at increasing security and autonomy. Finally, scenario analysis shows that today's undersea telecommunications system is highly exposed to disruption, especially in the East China Sea, the Indian Ocean, and the Mediterranean (Suez Strait).

Keywords: Geopolitical risk, decoupling, technological independence, internet, digital economy

*Porcellacchia: Kiel Institute (michael.porcellacchia@ifw-kiel.de); Trebesch: Kiel Institute and CEPR (christoph.trebesch@ifw-kiel.de); Wache: CPB Netherlands Bureau for Economic Policy Analysis and Kiel Institute (b.wache@cpb.nl). Christoph Trebesch acknowledges financial support from the European Union (ERC, Great.Power.Finance, 101087838). Views and opinions are those of the authors and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them. We thank Lorenzo Barrocu, Pietro Corti, Nicolo Di Luzio, Niklas Doehler, Matteo Frison, Federico Galletti, Jahana Jabbar, Sanskriti Jha, Alice Pontoglio, Mir Raisul Islam, Dean Sammanthan, Avi Shapiro, Joshua Sieberg, Tom Soytas, Thomas Tressel, Isabella Vornehm, Hannes Wehnhardt, Leonardo Vasquali, Yashvi Vohra, and Kexuan Zhou for excellent research assistance.

1 Introduction

Submarine cables are the arteries of the world economy. Between 95 and 99% of intercontinental data travels through a network of about 500 fiber-optic cables, with information passing oceans at the speed of light. These data flows sustain the digital economy, from AI and teleconferencing to cloud computing, as well as traditional sectors like finance, manufacturing, and logistics. Historically, cables have played a similarly critical role, as telegraphy enabled the rapid transmission of news, military orders, or financial transactions. Yet cables are also highly vulnerable to damage, sabotage, and political interference, as demonstrated by historical and recent incidents, e. g. near Taiwan and in the Baltic Sea. For these reasons, submarine cables represent a crucial chokepoint of globalization – since almost 200 years. Despite their critical role, however, undersea cables remain understudied.

This paper presents the first systematic effort to quantify the (geo-)economic significance and vulnerability of global telecommunications infrastructure, tracing both the present and the first era of globalization back to the 19th century. We focus on undersea cables because of their significance and because they allow analyzing the classic "security versus efficiency" trade-off in a rigorous way. The geographically fixed, international cable routes and their vulnerability to interference offers an ideal setting to study how geoeconomic forces shape the timing and geography of international investment and the evolution of global economic networks. Crucially, the geographic variation of these routes allows us to differentiate between cable investments driven primarily by economic incentives and those "strategic" cables that, while economically redundant, increase the security and independence of the cable owners.

We introduce the comprehensive, new *CableHist* dataset, covering the global, cross-border telecommunications infrastructure network over more than 150 years. For this purpose, we collect rich data on all international submarine cables, i.e. telegraphy, telephony, and internet, as well as every satellite launched into space. Beyond mapping the geography of cables, we code their technical specifications and, crucially, cable ownership. This enables us to conduct the first broad-based analysis of digital chokepoints in history and today.

To study the geoeconomics of subsea cables, we adapt a quantitative model of road traffic optimization to the context of telecom networks and data flows. This allows us to quantify two core dimensions. First, dependence (the extent to which data flows depend on cables controlled by allies or adversaries), and,

second, vulnerability (exposure to disruptions through cable cuts or sanctions). These measures enable a systematic quantification of each country's leverage and exposure in the global telecommunications system.

Conceptually, subsea telecom cables are a prototypical chokepoint. In the geoeconomics literature, a chokepoint is defined as a node in a network where the target has high dependence and few alternatives, creating leverage for coercion and exclusion (see Farrell and Newman, 2019; Clayton et al., 2026, 2025a; Fishman, 2025). Submarine cables fit this definition closely. First, economies worldwide crucially depend on data and information flows, but these flows are highly concentrated on a limited number of cables. Globally, there are a few hundred cables, but individual countries depend on far fewer (as of 2023, South Korea was connected to the world through just 10 fiber-optic cables, Taiwan through 12, Japan through 28, and Great Britain through 60). Second, a few large countries control a disproportionate share of this infrastructure, giving them high leverage for exclusion, surveillance, and sanctions against countries they seek to target.

Third, disruption is cheap while defense is expensive: a fishing vessel dragging an anchor suffices to cut a cable, while continuously surveilling thousands of kilometers of seabed is very costly. Repair capacity is equally constrained. Today there are only about 70 cable laying ships capable of repairing subsea cables, and just about 20 of them specialize in repairs (Subramanian, 2025; International Cable Protection Committee, 2025). In active conflict zones, such as the ongoing war theater in the Strait of Hormuz, repairs can be impossible altogether.

Finally, there are few viable alternatives to cables. Satellites are often seen as a substitute, but our data show they are a poor substitute due to their limited bandwidth and technical properties. For illustration, a single modern subsea cable can transmit up to 300 terabits per second. This is roughly equivalent to the combined capacity of *all* 7,000 SpaceX satellites currently in orbit. Satellites also face several technical constraints: they perform poorly in cloudy conditions, are vulnerable to electronic jamming, have higher latency (transmission times), and are more expensive to build and maintain. Their main comparative advantage lies in broad coverage, particularly in remote areas lacking cable infrastructure or reliable mobile networks.

The historical perspective of our study allows us to learn from the past and better assess the risks arising from close economic interdependence in times of tension and war. We provide evidence that security concerns have long influenced the design of telecom networks and global investment in critical infrastructure, especially during periods of great power rivalry (in line with earlier qualitative

work, e.g. by Headrick (1991)). We also document that powerful states have repeatedly weaponized their control over international telecom networks in the past, be it through exclusion, espionage, or the deliberate cutting of enemy cables.

In this light, the growing concerns about the weaponization of telecom infrastructure appear well-justified, as are current fears of "digital blockades" via cable sabotage or sanctions (see e.g. Farrell and Newman, 2023; Murphy and Pearl, 2025). As in past conflicts, multiple cable cuts —especially in active war zones — could overwhelm the world's limited fleet of repair ships, potentially leaving entire countries or regions offline for weeks or months. Our paper shows that today's debate on digital sovereignty and infrastructure protection is far better understood as part of a long historical continuum. More broadly, our review of the past 200 years shows that the discussion on security versus efficiency in globalized markets is far from new; it simply receded in the past three decades of relative geopolitical stability.

The main results of our paper can be summarized as follows:

1. **Hegemons dominate (and weaponize) global telecom networks**, first the UK and now the US. Our newly constructed dataset and the results of our traffic assignment model reveal how dominant large superpowers have been and continue to be in the international telecom market, and how dependent the rest of the world is on their infrastructure. In 1890, UK firms accounted for about 15% of global exports, but owned more than 50% of the international undersea cable network. Similarly, in 2024, the US accounted for just 10% of the world's exports, but US firms owned more than 25% of the global subsea cable system and 70% of all satellites in orbit.[1] We estimate that, in each hegemonic era, between a third and half of global data flows traveled through UK and US cables, respectively. Both superpowers also showed willingness to weaponize their control over global telecom networks, be it via (i) espionage, e.g. the UK's decryption of Germany's cables, or the US's cable espionage by the NSA, (ii) network exclusion. e.g. during colonial wars after 1890, or (iii) military sabotage in wartime, e.g. by cutting off the international data transmission of Germany in WW1 and of Japan in WW2.

[1] If we consider the G7 countries as a Western block then the numbers are 50% for cable ownership and 80% for satellites.

2. **Geopolitical risk spurs investment in new (economically redundant) cable systems**, especially by medium sized powers with bad or deteriorating relations with the dominant hegemon. We build on our traffic assignment model to estimate the drivers of new cable investments by country and find that geopolitical risks are a crucial driver of new investments, after controlling for economic incentives, market size and a range of fixed effects. We also find strong time patterns of decoupling: In peaceful times of open markets, smaller countries appear ready to use the telecom infrastructure owned by foreign nations, including by the hegemon. However, when geopolitical risk increases, we observe a trend to decoupling and self-sufficiency, especially for countries in rivalry with the hegemon. For example, prior to WW1, France, the US and Germany started to decouple from the UK and built their own international cable networks. Similarly, China has gradually decoupled from the US after 2010, with an estimated 60% of its international data flows now transmitted through Chinese-owned cables.

3. **Global data flows are highly vulnerable to cable cutting and sanctions.** Despite decoupling efforts and investments in economically redundant cables, the global telecom system remains highly vulnerable to disruptions. We estimate that cutting just 15 cables in the Mediterranean or the Pacific Ocean would disrupt around 10% of global data flows. Given historical precedents, and the rapid advancement of unmanned submarine technology, this is a very plausible scenario in case of conflicts. We show that island states such as Japan, the UK, or Taiwan are particularly vulnerable to the risk of cable disruptions.

Related literature: The paper relates to several strands of work. First, by studying digital chokepoints and the potential weaponization of critical infrastructure, we add to the small but fast-growing literature on geoeconomics, which has so far mainly focused on sanctions and embargoes in international trade and finance (see Clayton et al., 2025b; Mohr and Trebesch, 2025, for overviews). Our paper studies vulnerability and sabotage of physical infrastructure — a geoeconomic tool to project power that has been increasingly used, e.g. by China and Russia, in recent years[2], but which has not been quantitatively studied before in this literature.

[2]See e.g. The Economist, July 11, 2024: "How China and Russia could hobble the internet — The undersea cables that connect the world are becoming military targets."

Second, we contribute to the economic literature on telecommunication and information flows. The work by Steinwender (2018) and Juhász and Steinwender (2018) studies the rollout of international telegraphy cables and estimates their economic effects. More recently, Caoui and Steck (2025) structurally models bandwidth demand and cable entry on the modern subsea network, while Imbs and Pauwels (2026) characterize the topology and fragility of the fiber optic cable system since 2010. Our paper differs from these contributions by covering 175 years of cable and satellite infrastructure and by shifting the focus to the geoeconomic dimensions of the network: hegemonic dominance, the role of geopolitical risk in driving cable investments, and country level measures of dependence and vulnerability that incorporate ownership. See Hjort and Tian (2025) for a review on the economics of the internet.

Third, we contribute to the rich economic literature studying networks. We are not aware of existing work in this field that focuses on subsea cables or cross-border telecommunication infrastructure, despite their critical role for globalization. Instead, the existing literature mostly studies overland transportation networks such as highways and railroads (for a recent survey see Allen and Arkolakis, 2025). Recent work in trade and urban economics studies the economic impact of physical infrastructure on economic activity across space (e.g., Donaldson, 2018; Allen and Arkolakis, 2022; Fajgelbaum and Schaal, 2020). Another strand of literature uses methods from network theory to identify particularly central nodes within existing networks, e.g. in a pipeline network (e.g., Gallea et al., 2022). In contrast, we study dependence and vulnerability in the global telecom network by applying a traffic assignment model across every link (cable) in the network, which helps to estimate each country's risk and exposure to disruptions. In our empirical setting, ownership of parts of the network by different players is a central feature.

The remainder of the paper is structured as follows. Section 2 provides a historical and technical background on undersea telecom cables, in addition to a brief detour on satellites and an overview of past incidents of sabotage and espionage. Section 3 introduces the *CableHist* dataset, which covers all telecom cables. Section 4 outlines our traffic assignment model to measure dependence and vulnerability in global data flows. Section 5 presents a regression framework to study the security–efficiency trade-off. Section 6 discusses the main findings on hegemonic dominance, geopolitical drivers of cable investment, and vulnerability to disruption. Section 7 concludes.

2 Submarine cables: background and history

In the 21st century, near-instant global communication, enabling core aspects of the modern economy such as global value chains, e-commerce, high-frequency trading, and real-time teleconferencing, is taken for granted. But for most of history, communication was constrained by physical travel. Messages moved only as fast as horses, trains, or ships. Cross-border communication took days or even weeks. This began to change in 1850, with the first international submarine telegraph cable between England and France. Since then, the world has been transformed by a growing infrastructure of undersea cables and, more recently, satellites. Today's internet depends on around 500 submarine cables and several thousand satellites, built through both private and public investment.

In this section we briefly summarize the history of international telecommunication, with a particular focus on subsea cables and their (geo-)political disruptions and sabotage.

2.1 A primer on telegraph, telephone and internet cables, as well as satellites

The first permanent transatlantic cable started operations on July 27, 1866, after several prior, short-lived, and ultimately failed attempts. Over the next 40 years, telegraphy investments boomed and all major countries were connected to the growing global network, enabling same-day communication across much of the globe.

Since then, cable technology and bandwidth have advanced dramatically. Telegraph cables transmitted electrical pulses encoding Morse code, initially allowing only one message at a time and requiring manual decoding. Telephone cables allowed for analog voice transmission, later upgraded to digital signals, so that many simultaneous calls became possible, albeit with still limited capacity. In contrast to these earlier copper cables, today's fiber-optic cables use light to transmit massive volumes of data at near light speed, supporting millions of simultaneous connections. More specifically, in the 1890s, a typical transatlantic cable could transmit about 40 words per minute; by the 1950s, a typical cable supported 40 simultaneous phone calls, and 40,000 by the 1990s. Today's fiber-optic cables can transmit millions of high-quality video calls simultaneously. Remarkably, however, the basic principles of subsea cables have remained unchanged for over 150 years: cables are laid on the ocean floor, typically with a diameter similar to that of a garden hose (for a review of the history of telegraph cables

see Ahvenainen (1981, 1996, 2004, 2011)).

Satellites have also seen a remarkable technical evolution since the launch of Sputnik in 1957. Early models had limited bandwidth and short lifespans, used mainly for military surveillance as well as broadcasting. Today, thousands of active satellites provide global coverage for communication, navigation, and earth observation. A notable recent development is the rise of large low-earth orbit (LEO) constellations like SpaceX's Starlink, which offer lower latency (lower transmission delay) and higher bandwidth compared to traditional geostationary satellites — those that orbit at fixed positions relative to the face of the earth.

When comparing cables and satellites it is clear that subsea cables remain the dominant, indispensable backbone of international data transmission. The key limiting factor of satellites is bandwidth, with additional concerns about their sensitivity to weather conditions, high latency, electronic jamming, and high costs.

It is striking how much more powerful subsea cables are compared to satellites, despite satellites receiving far more attention in the media and public debate. The most advanced fiber-optic subsea systems, such as Google's transatlantic *Grace Hopper* or Facebook's 45.000 km long *2Africa* cable are each designed to carry 500–800 terabits (tbts) per second. This far exceeds the combined bandwidth capacity of all satellites currently in orbit. For example, Starlink's constellation of over 7000 satellites currently has an estimated combined capacity of about 350 tbts per second.[3] In addition, satellite lifespans typically average around 5 years, compared to 25 years or more for subsea cables.

These technical constraints and higher costs make satellites a complement rather than a substitute for submarine cables. One of the main advantage of satellites is their relatively good coverage in remote regions with no or limited cable connectivity (such as rural regions, or in the middle of the ocean), as well as in conflict regions such as Ukraine.

Compared to terrestrial fiber-optic cables, the building of undersea cables is also typically much more cost-effective in the case of international connections. Undersea cables avoid the often complex and time-consuming process of securing permits, navigating border crossings, and constructing infrastructure across densely populated areas. In contrast, subsea cables can often be laid along direct, uninterrupted paths across the seabed, thus bypassing the regulatory and physical obstacles that complicate overland construction.

[3]See Starlink's 2024 progress report `https://www.starlink.com/public-files/starlinkProgressReport_2024.pdf`.

While technological advances have increased submarine cable capacity, rising demand driven by cloud computing, generative AI, and video streaming has also significantly increased reliance on that capacity. As a result, the physical geography of submarine cables continues to constrain global data flows, and the disruption of even a single cable can have major consequences. In 2013, a severed cable near Alexandria caused a 60% drop in Egypt's internet speeds. In 2008, damage to key cables near Egypt disrupted services across the Middle East and South Asia, affecting up to 75 million users in India alone. In 2020, simultaneous faults in the WACS and SAT-3 cables caused widespread outages across West and Southern Africa, affecting tens of millions of people. More recently, in 2024, Houthi attacks in the Red Sea resulted in the severing of three subsea cables, disrupting access across East Africa and impacting an estimated 25% of European and South Asian internet traffic. These incidents reveal how submarine cables remain vulnerable chokepoints in the global internet infrastructure.

2.2 A brief history of digital blockades, espionage and sabotage of subsea cables

The physical characteristics of subsea cables make them vulnerable to accidental damage, but also to sabotage and espionage. This subsection provides a brief overview of well-documented cases of cable cutting, tapping, and sanctioning linked to political conflict, including periods of war. Important general sources for our case list include Kunert (1962), Headrick (1981, 1991), Sontag and Drew (1999), Winkler (2008), Kennedy (2014), Starosielski (2015), Giles (2016), Bruton (2017) as well as cable-specific documentation in our original sources, e.g. in the cable nomenclatures (see Section 3). A more comprehensive list of incidents will be included in future versions of the paper.

Two main takeaways emerge from our case review. First, throughout history, subsea cables have been repeatedly "weaponized" for geopolitical purposes — through sanctions, wire tapping, or cable cutting. Second, such actions have predominantly been carried out by great powers, in particular the UK and the US, but also China and Russia.

2.2.1 Sanctions and exclusion of geopolitical adversaries:

- *Telegraphy capture during the American Civil War (domestic cables):* During the American Civil War, the Union swiftly took control of much of the nation's telegraph network, effectively limiting the Confederacy's access.

Prior to the war, telegraph lines were operated by private companies like the American Telegraph Company and Western Union, facilitating domestic and some limited international communication. In 1861, the Union established the US Military Telegraph Corps, centralizing control and curtailing the South's ability to coordinate military operations. By seizing key telegraph hub, especially around Washington D.C., the Union secured a significant strategic advantage (Hochfelder, 2013; Wheeler, 2006).

- *The weaponization of telegraphy pre-WW1 (colonial wars):* In the late 19th century and the run-up to WW1, Great Britain increasingly exploited its dominance over global telegraphy to secure military and strategic advantages — prompting frustration and diplomatic protest from rival powers.
  - An illustrative case is the *Fashoda Incident* of 1898, when Britain and France confronted each other over territorial claims in the Upper Nile region (present-day South Sudan). British forces maintained direct telegraph access via a line running from Omdurman through Khartoum and Cairo to London, allowing for rapid military communication. In contrast, the French lacked their own telegraph connection, relying instead on slow couriers. During the incident, the British denied the French access to the telegraph line, resulting in an important strategic disadvantage. According to Headrick (1991), British commander General Kitchener transmitted selectively negative information about the French position, leading to a misperception in Paris that Marchand's expedition was in serious difficulty. This contributed to their decision to back down.
  - A far more consequential cable blockade occurred during the *Boer War* (1899–1902), when Britain fought against the Boer republics of Transvaal and the Orange Free State. Beginning in October 1899, British authorities implemented strict censorship, re-routing, and outright blocking of telegraph traffic to and from southern Africa. The primary aim was to suppress independent war reporting and disrupt diplomatic communications between the Boers and their European sympathizers. The ban was so broad that it prohibited the transmission of any ciphered or foreign-language telegram south of Aden, forcing such messages to pass through London for approval or redaction. As a result, the cable blockade also curtailed French and German communication with their own African colonies, prompting formal diplomatic

protests and ongoing criticism from European governments.

  - *Britain's offensive cable strategy pre-WW1:* Following Fashoda and the Boer war, British strategic thinking increasingly evolved towards actively exploiting its dominance over global telecommunications. This shift was facilitated by the completion of the "All Red Line" in 1902 — an extensive global network of submarine cables connecting British territories without relying on foreign cables or stations. Britain's intent to weaponize its cable dominance was codified in key policy documents, including the 1904 *Memorandum on the Protection of British Submarine Cables and on the Destruction of the Enemy's Cables*, which outlined plans to disrupt adversaries' cable networks. The 1911 report *Submarine Cable Communications in Times of War* further detailed Britain's options to control communications, intercept enemy messages, isolate rival powers, and build resilience.

- *Soviet exclusion during the Cold War:* During the Cold War, the US and the UK effectively excluded the Soviet Union and its allies from accessing the growing, Western-controlled global submarine cable network, as well as the INTELSAT satellite system. While not subject to a formal telecommunications embargo, the Soviet bloc could therefore not engage in global telecommunication via Western routes. In addition, the export of advanced telecommunications technologies was tightly controlled via mechanisms such as the Coordinating Committee for Multilateral Export Controls (CoCom). As a result, the USSR had to rely on intra-bloc terrestrial cables, radio communications, and its own satellite systems such as Molniya and Gorizont, which were similarly off-limits to Western nations (Peters, 2016; Bertsch, ed, 1988).

- *Digital embargo of Cuba:* Cuba has long faced a telecommunications and cable embargo, severely restricting its telephony and internet access. After the 1959 revolution, the US banned cable links with Cuba and later imposed strict export controls on telecom technologies, along with more recent restrictions on internet services such as Google Earth, Zoom, and Amazon. Our data show that all US-owned cables in the Gulf of Mexico and the Caribbean bypass Cuba. Consequently, until the mid-2000's, Cuba could access the internet solely via geostationary satellites, at high costs and limited bandwidth. It was not until 2013 that Cuba connected to a subsea fiber-optic cable via Venezuela, followed by a second link to Martinique

in 2023. Although the US lifted its cable-laying ban in 2016, Cuba's 2022 request to access the US-owned ARCOS-1 system was denied by the US authorities on national security grounds.

2.2.2 Espionage in peacetime and war:

- *British wiretapping in WW1 (& Zimmermann Telegram):* During WW1, British intelligence systematically tapped undersea telegraph cables by accessing landing sites like Porthcurno and intercepting messages at relay stations in London or Cornwall. After the UK cut all of Germany's direct cables to the Americas (see below), German messages could only be transmitted via neutral countries, enabling interception at British-controlled hubs, or high-powered radio communication, which could be deciphered. This decryption was handled by Room 40, a secret Admiralty unit specializing in naval and diplomatic codebreaking. A major success was the interception of the Zimmermann Telegram, in which Germany proposed a military alliance with Mexico against the US. The interception and decryption of this telegram helped to shift American opinion toward entering the war against Germany (Hinsley, 1979).

- *British and US communication espionage in WW2:* During WW2, Allied intelligence services — primarily Britain's Bletchley Park and the US Signal Intelligence Service — intercepted both high-frequency radio and undersea cable traffic used by Axis powers. These channels carried encrypted communications on military logistics, troop movements, and diplomacy. A major breakthrough came with the decryption of German Enigma traffic under the ULTRA program, which significantly aided the Allies (Andrew, 2010).

- *Cold War espionage I — Operation Ivy Bells (1971-1981)*: In 1971, operatives of the US Navy and National Security Agency (NSA) covertly tapped a Soviet undersea communications cable in the Sea of Okhotsk. The cable transmitted sensitive information between the Soviet Pacific Fleet headquarters in Vladivostok and naval installations on the Kamchatka Peninsula. The operation yielded high-value intelligence on Soviet naval strategy and submarine deployments for nearly a decade, until it was compromised by former NSA contractor Ronald Pelton in 1980 (Craven, 2002; Sontag and Drew, 1999).

- *Cold War espionage II — the ECHELON program (Five Eyes):* Established in the 1970's, the ECHELON program — operated by the Five Eyes alliance (USA, UK, Canada, Australia, New Zealand) — was designed to intercept global communications for signals intelligence, initially targeting the Soviet bloc. The system primarily intercepted satellite transmissions, but also gathered data from international cable networks where signals were routed through key landing points. Over time, ECHELON expanded its collection to include a wide range of diplomatic, commercial, and military communications worldwide (Bamford, 2002; Aldrich, 2011).

- *The NSA Tempora program tapping internet cables (ca. 2009-2013):* Revealed by Edward Snowden in 2013, the NSA and UK's GCHQ tapped into fiber optic subsea cables at landing stations to collect vast amounts of internet and telephone data. By accessing cable data streams directly, these agencies gained unprecedented surveillance capabilities. The case underscores the scale and technical sophistication of modern cable-based espionage. Other key NSA programs involving international subsea cable interception include MUSCULAR, which tapped private fiber links between major data centers operated by Google and Yahoo, and Fairview, which targeted international communications carried through US infrastructure, including subsea cable landing stations.

2.2.3 Cable cutting and sabotage:

By systematically searching archives, scientific literature, and online sources for historical cable cutting cases, we identified at least 91 incidents of attempted or successful subsea cable cutting up to 1945, which should be seen as a lower bound. We find that until the end of WW2, reported cases of subsea cable cutting appeared almost exclusively as outright acts of war during major conflicts. This changed during the Cold War, when the US and the Soviet Union prioritized espionage over outright sabotage and the boundaries between deliberate aggression and accidental damage became increasingly blurred by "gray-zone" attacks.

- *Sabotage in the Spanish-American War:* One of the earliest conflicts in which cable cutting became a central strategic instrument was the Spanish-American War of 1898. Well before hostilities began, US Navy planners had recognized the military importance of the telegraph cables connecting Spain to its colonies in Central America (Kimball, 1896). Once the conflict started,

the US Navy systematically severed Spanish telegraph lines around Cuba and the Caribbean. Our data record at least 19 attempted or successful cable cuts. These operations successfully disconnected the Spanish colonies of Cuba and Puerto Rico from Madrid, depriving Spain of command and control over its forces and giving the United States a decisive advantage.[4]"

- *Sabotage in WW1:* In August 1914, the Royal British Navy successfully severed the main telegraph cables that linked Germany to the rest of the world, in particular those running through the English Channel to the US, Brest, Vigo, the Azores, and Tenerife (Kunert, 1962).[5] For the remainder of the war, Germany had only limited means to communicate or transfer funds internationally, including with its overseas territories and allies, but also to counter the intense propaganda which the UK transmitted to the US.

  Germany retaliated by cutting the Baltic Sea cables that connected Britain and France with Russia (Winkler, 2008). Moreover, towards the end of the war, Germany started to deploy submarines to sever cables and threaten repair ships (O'Connell, 2010). This strategy proved increasingly effective: the Atlantic became a telegraphy bottleneck in which commercial, diplomatic, and military traffic competed for dwindling capacity. According to historians, this experience prompted the United States to invest heavily in building its own international cable infrastructure and radio technology (Winkler, 2008).

- *Sabotage in WW2:* Similar to WW1, the belligerents of WW2 spent considerable resources to disrupt one another's submarine cable networks. A central objective of these operations was to force the enemy to rely on radio communication (wireless telegraphy), which was widely used in this period but much easier to intercept than cable communication. In 1939, the British successfully cut German cables from Emden to Spain, Portugal and the US (via the Azores), followed by those linking the German islands of Borkum and Norderney with England and Norway. During the first year of the war, there were at least 25 incidents of cable cutting or attempted cable cutting

[4]Insightful sources on this episode include United States. Navy Department. Bureau of Navigation (1898), Goodrich (1900), Goodrich (1904), Wilson (1900), and Allen (1898).

[5]These operations were based on prewar plans in which the Royal Navy identified the most important German telegraph lines to be cut. Further, Great Britain occupied or destroyed telegraph stations like the one on Yap Island, which was crucial for Germany's Pacific communication (Winkler, 2008).

of German cables in the English Channel, the North Sea and the Atlantic. The British also launched several operations against Italy and Japan, in particular by cutting Italy's cables in the Atlantic and Mediterranean and severing multiple Japanese lines.[6] While Germany largely refrained from cable cutting, Italy cut all British cables around Malta and Gibraltar and Japan captured and cut British cables in the Far East (Bragadin, 1957). Towards the end of the war in the Pacific, specially developed Australian midget submarines cut the remaining Japanese cables to Saigon, Singapore and Hong-Kong to enforce the use of radio communication ("Operation Foil" and "Operation Sabre") (Naval Association of Australia, 2020). These operations were militarily crucial, as it allowed the US to intercept Japan's strategic planning prior to dropping the atomic bombs in August 1945 (Department of Veterans' Affairs, 2024).

- *Sabotage in the Cold War:* After 1945, deliberate cable cutting between adversaries became less common, as major powers such as the US and the Soviet Union prioritized espionage over outright sabotage (see below). A notable exception is the 1959 Novorossiysk incident, in which the US Navy boarded a Soviet fishing trawler suspected of having cut five transatlantic cables operated by AT&T and Western Union, roughly 120 miles off the coast of St. John's, Newfoundland.

- *Baltic and Northern Sea incidents since 2022:* In the wake of the escalating tensions and Russia's full-scale invasion of Ukraine in 2022, both the concerns over and actual cable cutting incidents in Northern Europe increased.[7] In Jan. 2022, the fiber-optic Svalbard Cable, owned by Space Norway and connecting mainland Norway to the Arctic island of Svalbard, was severed, reportedly by Russian fishing vessels (Conley et al., 2024). Svalbard is in a strategic location and hosts the SvalSat antenna park, the world's largest satellite ground station serving NASA, ESA, and others. In Oct. 2023, the Chinese-flagged vessel NewNew Polar Bear reportedly damaged two subsea cables linking Estonia with Finland and Sweden (Conley et al., 2024). In Nov. 2024, Finland's key C-Lion1 cable to Germany and the BCS East-West cable between Sweden's Gotland Island and Lithuania were

[6] The most valuable sources for British WW2 cable cutting are the Royal Navy's War Diaries: Royal Navy (n.d.)

[7] For an excellent overview of the debate and the known facts see the collection of articles by the Carnegie Endownment: `https://carnegieendowment.org/the-geopolitics-of-subsea-data-cables?lang=en`.

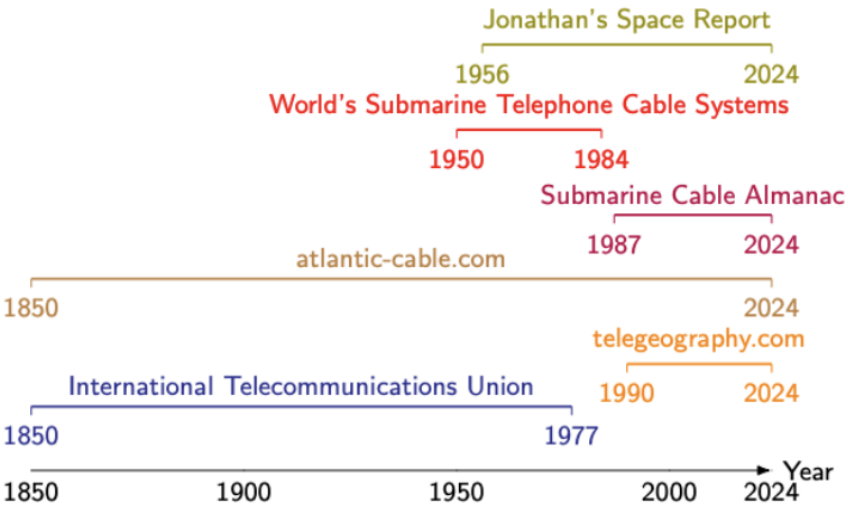
severed, reportedly by the Chinese-flagged Yi Peng 3 carrying Russian fertilizer (Sutherland, 2025). Relatedly, in Dec. 2024 the Estlink 2 Power Cable connecting Finland and Estonia and four telecom cables were cut by the Cook Islands-flagged Eagle S that was linked to Russia's "shadow fleet"(Sutherland, 2025). In Dec. 2025, three additional cables were cut or damaged, suspectedly by a Russian cargo ship. While these incidents all involved ships linked to China and Russia, there is insufficient proof they were deliberate or politically ordered. However, they are often seen as part of a broader strategy of "gray-zone" or "hybrid" warfare (Farrell and Newman, 2023).

- *Taiwan incidents in recent years:* Taiwan has long blamed China for repeatedly damaging the subsea cables connecting the island to the outside world. Recent examples include the Matsu Island incident In February 2023, the only two cables to Matsu were severed, reportedly by a Chinese fishing vessel and a cargo ship, disrupting internet access for the island's 14,000 inhabitants for several weeks (Ocon and Walberg, 2025). In January 2025, the Shunxing 39, a Chinese-crewed cargo ship, was suspected of damaging a subsea cable linking Taiwan to the US (Ocon and Walberg, 2025). Later, in February 2025, the Hongtai 58, also with a Chinese crew, was detained following the damage of a cable connecting Taiwan to the Penghu Islands (Ocon and Walberg, 2025). Similar to incidents in the Baltic Sea, a proof of deliberate sabotage is difficult, but Taiwanese authorities consider it likely (Murphy and Pearl, 2025).

3 The CableHist dataset — mapping the global telecom network 1850-2025

This project introduces the *CableHist* dataset. It is the first database reconstructing a systematic history of every known international cable ever laid under the sea, and every telecommunication satellite ever launched into space. *CableHist* considerably expands on existing datasets with information from several primary sources which were digitized and coded by our research team in the span of more than three years. Figure 1 gives an overview of the sources used in constructing the database. The result is a database with detailed information on the technological, geographic, and economic characteristics of these critical pieces of infrastructure, providing a granular perspective on the historical evo-

Figure 1: CableHist: data sources and coverage



lution of one of the most extraordinary achievements of mankind — the global telecommunication network.

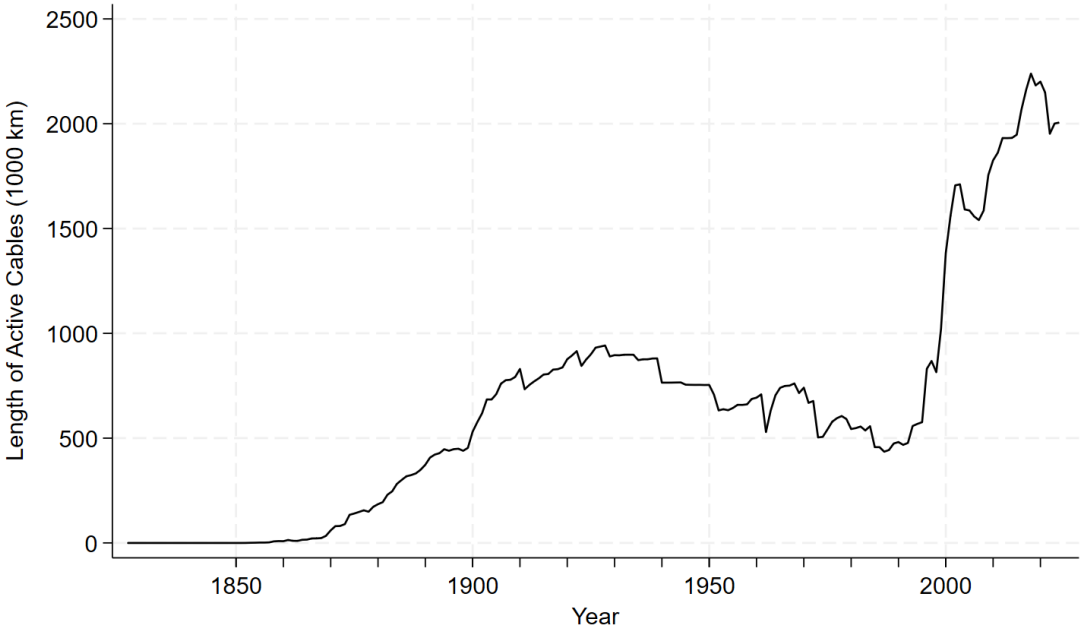
The database is the result of several years of manual data collection and synthesis. The full database currently covers 1,773 cable systems in history and today, with a total length of 2.7 million kilometers, 544 owning entities, and unique 2,935 landing points, as well as 21,234 satellites. Note that cable systems typically consist of several individual cables, i.e. cable segments. The earliest cable in the database is recorded in 1850, with the latest becoming active in 2025. Of the cable systems, 1,054 are active in the telegraph era (before 1950), 349 are active in the telephone era (1951 - 1994), and 370 are active in the internet era (1995 - 2025).

We will supplement the paper in the future with an Online Appendix, detailing the database and its construction, and we will also make the database available for other researchers.

3.1 Underwater Cables (Telegraph, Telephone, Internet), 1850-2025

In the cables section of *CableHist*, we aim to cover the history of every international submarine telecommunication cable ever built. For each cable, the database records the dates of its entry into and exit from service, its geography (i.e. the places that it connected), which firms were involved in its construction, operation,

Figure 2: Total length of active cables per year



and maintenance, the distribution of its ownership, the construction costs, the cable's capacity, and other technical features. Figure 2 gives an overview of the total active extent of the cables network across time.

The database is constructed manually from the underlying sources. We first coded each source independently, before combining them into a consensus database, containing the most authoritative version of each cable. The choice between following different sources was made case by case, weighing factors like kind of source (official, commercial, personal), date of source (contemporary or later), and other factors.

The database has limitations in some dimensions, mostly due to lack of availability of source material. It was particularly difficult to find systematic cable-level data on exact ownership shares of different owner entities per cable

system[8], costs of building[9], out-of-service dates[10], and bandwidth[11].

The cables database consists of five datasets:

- *Cables*: time-invariant features of cables
- *Landing points*: geographic information about every landing point of every cable
- *Capacities*: information on the capacities of each cable over time
- *Companies*: information on every company or government that was ever involved with a cable (owners, suppliers, operators, etc.)
- *Ownerships*: linking owners to cables across time

Data Sources. Given the wide time coverage of the database on cables, we must rely on several sources, some produced by official bodies, some by research companies, and others by volunteers and enthusiasts. The combination of all of these sources enables us to produce the most comprehensive and detailed database on international submarine cables. The only existing source which spans from the first telegraphy cables to the latest internet cables is *Atlantic Cable*, a freely accessible website. However, because the historical coverage of *Atlantic Cable* is limited, we also include information from the *Nomenclature des câbles formant le réseau sous-marin du globe* These documents are the results of a series of censuses of submarine cables performed (roughly) every five years between 1877 and 1977 by the International Telecommunication Union (ITU). Additionally, we add information from the *World's Submarine Telephone Cable Systems*, a source curated by the US Department of Commerce between 1950

[8]Ownership shares that are different from 0, 50, or 100% are a relatively recent phenomenon, emerging mostly since around the 1990's, in the era of large-scale inter-continental cable systems frequently operated by groups of owners. In cases of unobserved ownership shares, we currently assume equal ownership of the unknown ownership portion between known owners.

[9]This variable can be approximated reasonably well, but precise cable-level costs of building are not always available.

[10]Ready-for-service dates are frequently observed and explicitly recorded for each cable, while out-of-service dates can sometimes only be bounded, e.g. in cases where a given cable is known to have gone out of service between the publishing of two subsequent censuses. In the absence of more specific cable-level information, we assume that a cable stays active until 25 years after the last time we observe that it is active.

[11]Especially for modern fiber-optic cables, the difference between potential capacity (i.e. the maximum theoretical capacity) and lit capacity (the capacity enabled by the hardware currently installed on either side of the cable) is important. Typically, information on potential capacity is more readily available than information on lit capacity, since lit capacity can frequently change for the same cable over time. The same distinction can be made for telegraph cables, albeit this is less of an issue.

and 1990. We further use additional information from a proprietary dataset on submarine cables maintained by *Telegeography*, one of the leading research companies on international telecommunications.[12] Our final source is the *Submarine Cables Almanac* by *SubTel Forum*, an ongoing effort started in 2011 with the aim to perform quarterly censuses of every active international submarine cable.

3.2 Satellites, 1957-2025

The satellites part of *CableHist* covers the history of every satellite that was ever used for commercial telecommunication. For each satellite, the database records the dates of its entry into and exit from service, details on its orbit, which firms and government agencies were involved in its construction, launch, operation, and maintenance, the distribution of its ownership, and other technical features. As future steps, we will also add information on every satellite's footprint (the geographic region covered by its signal), the construction and launch costs, and the satellite's capacity.

Similar to the cables part of the database, the satellites part of the database is also structured into five datasets:

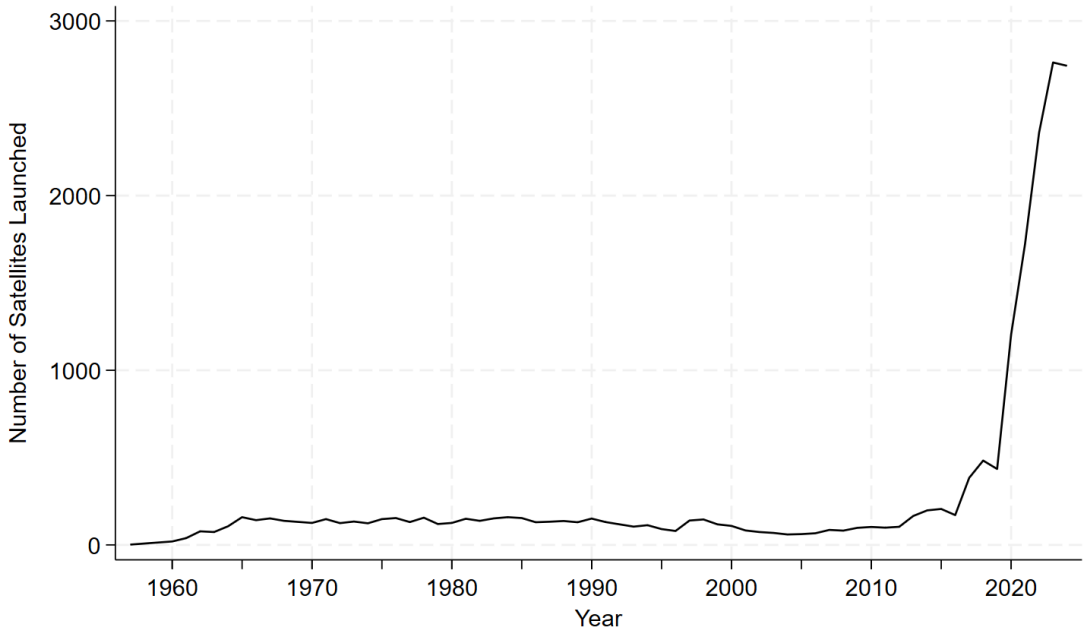
- *Satellites*: time-invariant features of satellites
- *Orbits*: orbital information that can be used to calculate the satellite's geographic coverage
- *Capacities*: information on the capacities of each satellite across time
- *Companies*: information on every company or government that was ever involved with a satellite (owners, suppliers, space agencies, etc.)
- *Ownerships*: linking owners to satellites across time

Data Sources. Our main data source on satellites, covering our entire sample period, is the *General Catalog of Artificial Space Objects (GCAT)* by Jonathan C. McDowell. This dataset contains information on the technical aspects of satellites, their out-of-service dates and ownership changes. We use two complementary data sources. First, the *Table of Artificial Satellites Launched*, periodically published by the ITU between 1967 and 1993. This source includes detailed information on every satellite launched before 1993. Second, the Czech Academy of Sciences curates a website with detailed technical data about every satellite that was

[12] Telegeography's EULA does not allow redistribution of the underlying data.

launched into space between 1957 and 2012, including information about their bandwidth and capacity.

Figure 3: Number of satellite launches by year



4 Quantifying traffic, dependence, and vulnerability in the telecommunications network

A central objective of our empirical analysis is to quantify the economic incentives of cable investments as well as every country's exposure to cable-related geopolitical risks, e.g., espionage, sabotage, or sanctions. To this end, we analyze a simple traffic assignment model which determines how data flows traverse the global telecommunication infrastructure.

Methodologically, we build on a rich and established literature in network economics. Several earlier papers estimate traffic flows via a shortest-path algorithm like we do, for example, Donaldson (2018) for Indian railroad expansion, Allen and Arkolakis (2014, 2022) for the US interstate highway system, Fajgelbaum and Schaal (2020) for road networks in Europe, or Arkolakis and Walsh (2023) for global electricity transmission networks.

These papers all have one thing in common: they study the benefits of expanding a given network. Our approach differs fundamentally in that we focus on disruptions to the network rather than its expansion. This section

outlines the approach in detail and explains our newly developed measures of network dependence and vulnerability.

4.1 Traffic Assignment Model

The telecommunication network is a set of nodes N and links L where we interpret nodes as countries that exchange data with each other and links as submarine or terrestrial corridors in which telecommunication cables are built (e.g., trans-Atlantic, trans-Pacific, etc.).[13] In general, the problem of determining how flows between nodes are routed on a network's links is known as a traffic assignment problem. The key ingredients of any such problem are:

- An OD (origin-destination) matrix $(Flow_{od})_{o\in I,d\in I}$, where each component, $Flow_{od} \geq 0$, specifies the volume of data flows between country o and d. As we discuss in the Appendix, we proxy data flows with bilateral trade flows.
- A transportation cost vector $(Distance_\ell)_{\ell\in L}$, where each entry, $Distance_\ell \geq 0$, determines the cost of sending or receiving each unit of data flow via corridor ℓ. Figure 4 offers a visual representation of the main corridors we consider.[14]

Let $p(o,d) \subseteq L$ be a path connecting country o and d, i.e., a sequence of corridors connected to each other and to the given country pair, and let $\mathcal{P}(o,d)$ be the collection of all such paths. We assume that data flows are routed on the path that minimizes the transportation cost of delivering data from o to d. Formally, we assume that flows between o and d are routed on path $\hat{p}(o,d)$ such that

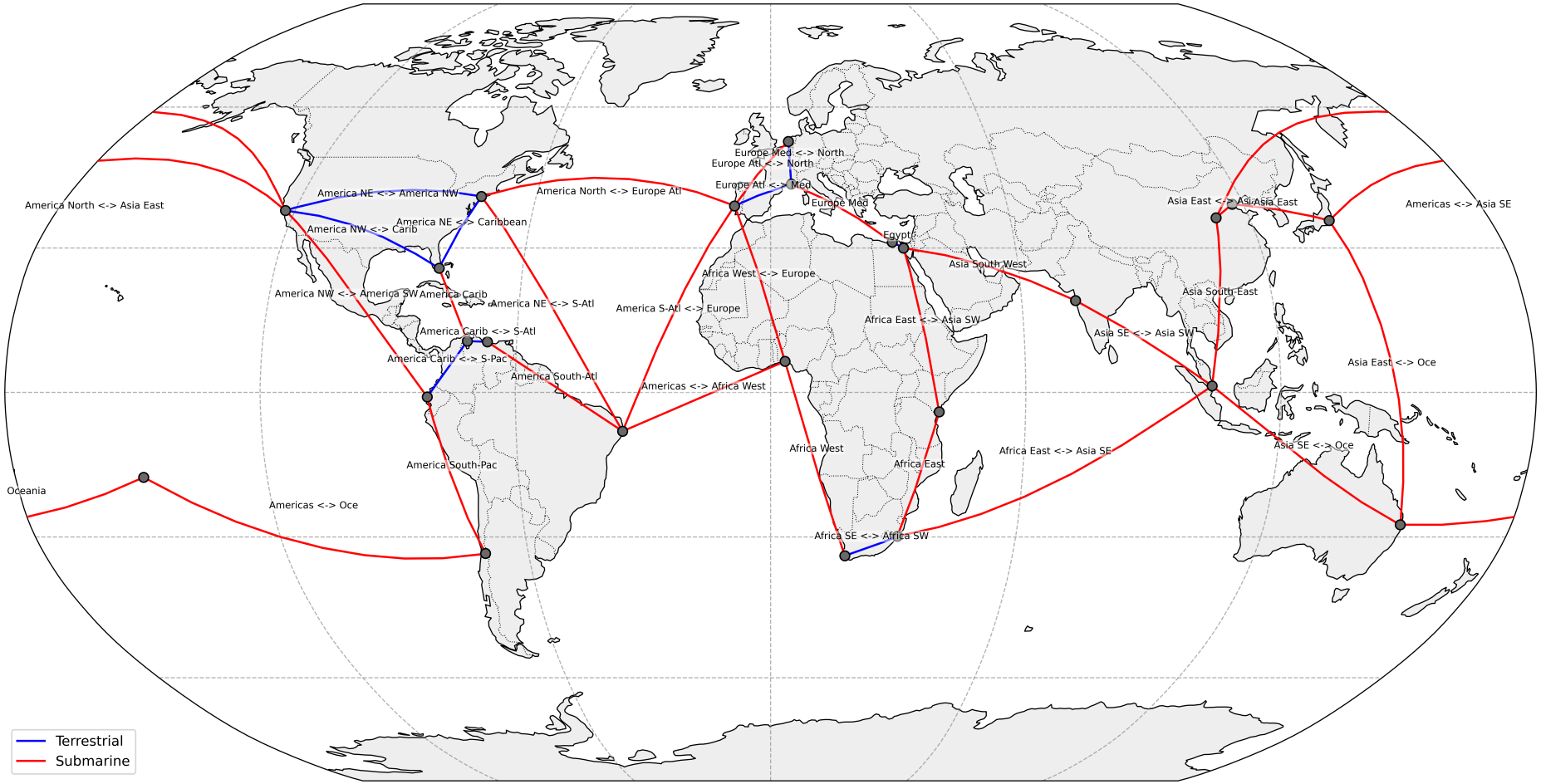
$$\hat{p}(o,d) \in \arg\min_{p\in\mathcal{P}(o,d)} \sum_{\ell\in p} Distance_\ell$$

To simplify the notation (and to reflect the realities of our empirical network), we assume that the solution to the problem above is unique for every country

[13] As we explain in the Appendix, we follow Fajgerlbaum and Schaal (2020) and focus on corridors rather than individual cables before applying our shortest-path assignment.

[14] We also assume that each pair of countries sharing a land border can exchange data via a reserved terrestrial corridor. In the appendix we explain the full set of corridors we consider, we define their costs, and discuss how we relate them to cables.

Figure 4: Map of global corridor network



pair. Finally, for every two countries o and d and corridor ℓ we define

$$\pi(\ell, o, d) := \begin{cases} 1 & \text{if} \quad \ell \in \hat{p}(o, d) \\ 0 & \text{if} \quad \ell \notin \hat{p}(o, d) \end{cases}$$

This function indicates whether corridor ℓ is part of the shortest path connecting o and d.

Note that the shortest-path assumption implies that all the data exchanged between o and d will be routed on one path only, even if it is only marginally less costly than alternatives. This simplifying assumption, which is standard in the literature, would be too strong for the network of cables whose density implies that there are many alternative paths with similar costs. However, in our exercise, we are focusing on the (much smaller) network of submarine and terrestrial corridors where different paths have relatively large differences in costs.

4.2 Global and Domestic Traffic

A simple approach to measure the economic value of building a particular cable is to assume that profitability is increasing in predicted cable use. As cables are built on corridors, we must first determine which corridors are used more. To this end, we note that given the OD matrix of data flows, our shortest-path assumption pins down a traffic vector $(Traffic_\ell)_{\ell \in L}$ representing how much of the data flows is routed on corridor ℓ. Formally, traffic on corridor ℓ is given by

$$Traffic_\ell = \sum_{o \in I} \sum_{d \in I} \pi(\ell, o, d) Flow_{od}$$

From the perspective of country i, the vector of domestic traffic, $(Traffic^i_\ell)_{\ell \in L}$, i.e., the traffic generated by the data flows that come from or go to country i, is such that, for each $\ell \in L$,

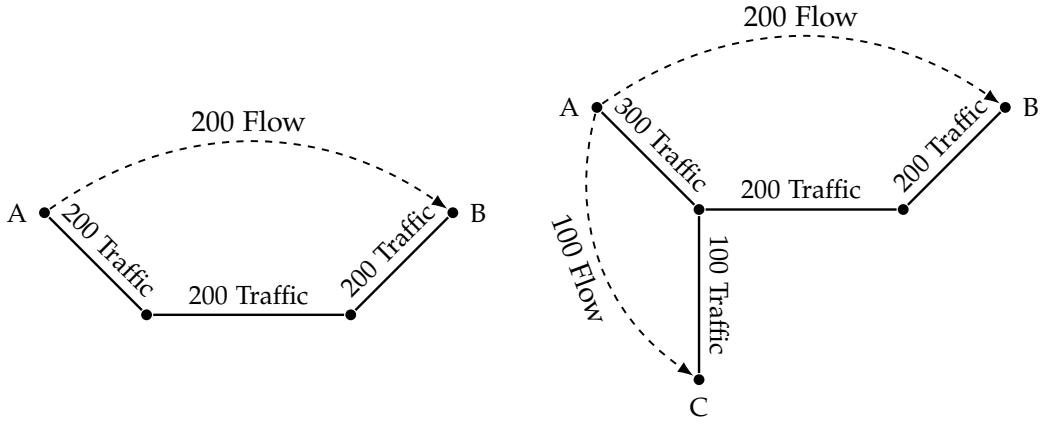
$$Traffic^i_\ell = \sum_{d \in I} \pi(\ell, i, d) Flow_{id} + \sum_{o \in I} \pi(\ell, o, i) Flow_{oi} = \sum_{j \in I} \pi(\ell, i, j) [Flow_{ij} + Flow_{ji}]$$

where the last equality is due to the symmetry in the cost of receiving and sending data via each corridor ℓ (implying $\pi(\ell, i, j) = \pi(\ell, j, i)$).

Figure 5 shows a graphical representation of a traffic assignment in two simple network configurations. On the left we see a network with only two nodes, A

and B, and the OD matrix consists of just one non-zero entry ($Flow_{AB} = 200$). Given that only one path between A and B exists, we know that each link along that path must carry all of the data flows. As a consequence, we have $Traffic_\ell = 200$ for each link ℓ. On the right, instead, we modify the network by including an additional node C and a new link connecting C to the previous network. Additionally, the OD matrix now also includes a new non-zero term, $Flow_{AC} = 100$. If traversing each link has non-zero costs, then the shortest path assumption would predict the traffic assignment displayed in the picture. As we can see, the link closest to A now carries 300 units of traffic, as it is used to carry all data flows from and to A.

Figure 5: Graphical representation of Traffic Assignment



We interpret $Traffic_\ell$ as a variable affecting the profitability of building a cable in corridor ℓ for any provider of connectivity. Instead, domestic traffic $Traffic^i_\ell$ represents the domestic interest of country i in the connectivity offered in corridor ℓ. If we assume that connectivity providers from country i are able to extract higher profits from customers in country i, then we can interpret $Traffic^i_\ell$ as a variable capturing a country-level corridor-specific measure of profitability. Otherwise, it can be interpreted as an index of i's national interest in corridor ℓ, which might translate into subsidies offered by country i to any connectivity provider willing to invest in corridor ℓ.

4.3 Vulnerability

We think of vulnerability as the risk of data flow disruptions due to cable ruptures or sabotages. To define this concept formally, we introduce parameter $NumCables_\ell$ which measures the number of cables active on corridor ℓ. Addi-

tionally, we define total data flows as $GlobalFlows = \sum_{o \in I} \sum_{d \in I} Flow_{od}$. With this, we define global vulnerability to corridor ℓ as:

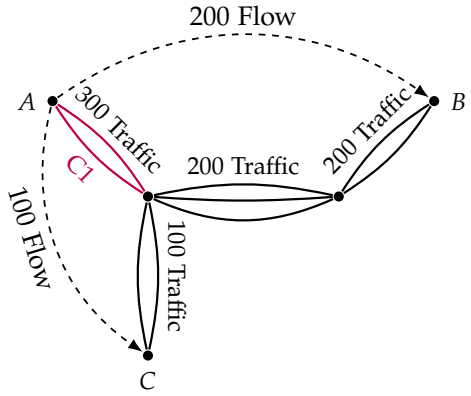
$$GlobalVulnerability^{\ell} = \frac{Traffic_{\ell}}{NumCables_{\ell} \cdot GlobalFlows} \in [0, 1]$$

Vulnerability increases when a larger share of global data flows transits on a corridor or when the number of cables in that corridor diminishes.

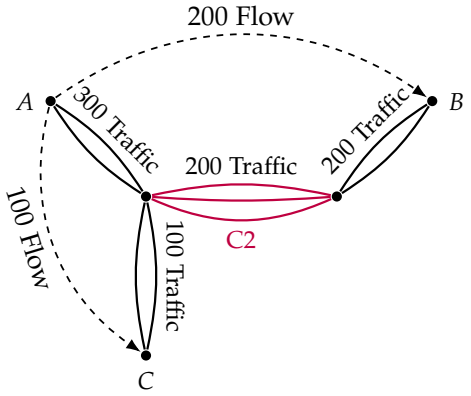
Figure 6 provides a visual representation of vulnerability. Note that, relative to Figure 5, we enriched the network structure by duplicating each link multiple times: each duplicated link represents a distinct cable in a particular corridor ($C1$, $C2$, $C3$, or $C4$). Figure 6 reports global vulnerability on each of the four corridors. As we would naturally expect, global vulnerability is largest in corridor $C1$ as such corridor carries all of the data flows and it only consists of two cables. The idea is that if either of these cables breaks, then 50% of all data flows would be affected.

Figure 6: Graphical representation of Vulnerability

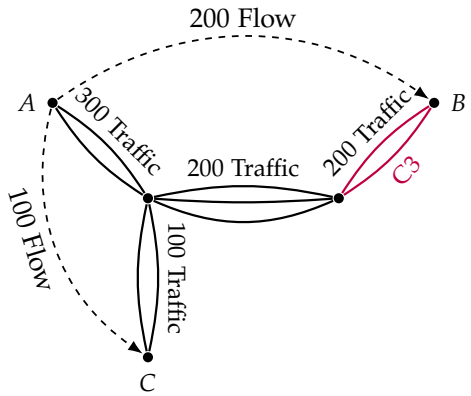
(a) $GlobalVulnerability^{C1} = \frac{1/2 \times 300}{300} = 50\%$



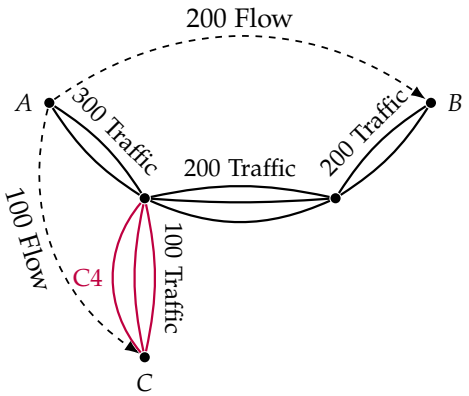
(b) $GlobalVulnerability^{C2} = \frac{1/3 \times 200}{300} \approx 22\%$



(c) $GlobalVulnerability^{C3} = \frac{1/2 \times 200}{300} \approx 33\%$



(d) $GlobalVulnerability^{C4} = \frac{1/2 \times 100}{300} \approx 17\%$



In this sense, we can think of corridors with high global vulnerability as digital chokepoints of the global economy. Still, it is important to note that global vulnerability masks important country-level heterogeneity and asymmetries. For example, the corridor connecting North America to Europe is an important chokepoint for Europe or North America, as it channels all data flows between the two regions, but it carries very few of China's domestic flows (if any). To capture this heterogeneity, we let $TotFlows^i = \sum_{d \in I} Flows_{id} + \sum_{o \in I} Flows_{oi}$ and we define country i's vulnerability to corridor ℓ as

$$Vulnerability_i^\ell = \frac{Traffic_\ell^i}{NumCables_\ell \cdot TotFlows^i} \in [0,1]$$

A country is highly vulnerable to a corridor when a large share of its data flows transits on a corridor with limited cable redundancy. In the previous example, the United States and Germany would be much more vulnerable to the trans-Atlantic corridor than China.

4.4 Dependence

Lastly, we capture country i's *dependence* on country s as the extent to which i relies on infrastructure owned or controlled by s.

We denote by $NumCables_\ell^s$ the number of cables in corridor ℓ that are owned (at least in part) by country s, and we define the dependence of country i on country s as

$$Dependence_i^s = \sum_{j \in I} \left(\max_{\ell \in L} \pi(\ell, i, j) \frac{NumCables_\ell^s}{NumCables_\ell} \right) \left[\frac{Flow_{ij} + Flow_{ji}}{TotFlows^i} \right] \in [0,1]$$

Similarly, we define global dependence as

$$GlobalDependence^s = \sum_{i \in I} \sum_{j \in I} \left(\max_{\ell \in L} \pi(\ell, i, j) \frac{NumCables_\ell^s}{NumCables_\ell} \right) \left[\frac{Flow_{ij}}{GlobalFlows} \right] \in [0,1]$$

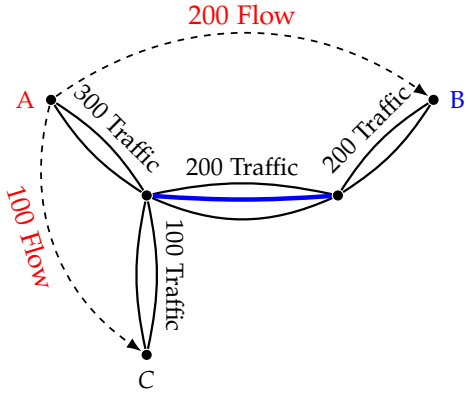
Note that, $\frac{NumCables_\ell^s}{NumCables_\ell}$ is the share of cables in corridor ℓ controlled by country s. Moreover, recall that $\pi(\ell, i, j) = 0$ if ℓ is not part of the path connecting i and j and $\pi(\ell, i, j) = 1$ otherwise. With this in mind, we see that both dependence measures are weighted averages of bilateral flows (divided by total flows) where the weights are given by the maximum ownership share of country s among all corridors that carry $Flow_{ij}$. In this sense, dependence captures the share of

country i's data flows that are exposed to unilateral action or surveillance by country s.

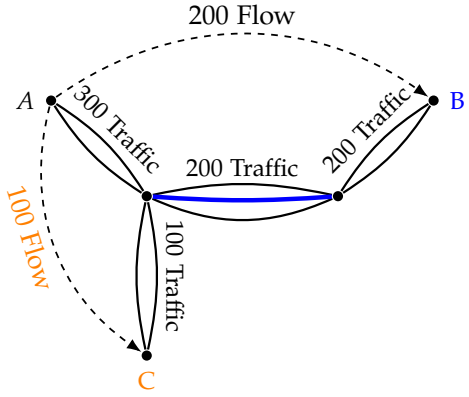
Figure 7 shows some examples of dependence. As we can see from the definitions above, to calculate dependence we need a notion of ownership; in the figure, each blue line represents a cable owned by node B. Figures 7a and 7b show dependence of node A on B and of C on B, respectively, for the case where B only owns $1/3$ of the cables in the path between A and B. As we can see, C's dependence on B is zero, as none of its flows are routed on B's cables. On the other hand, $2/3$ of A's flows are routed on a link in which B owns $1/3$ of the cables. As a consequence, B's dependence on C is $2/9 \approx 22\%$.

Figure 7: Graphical representation of Dependence

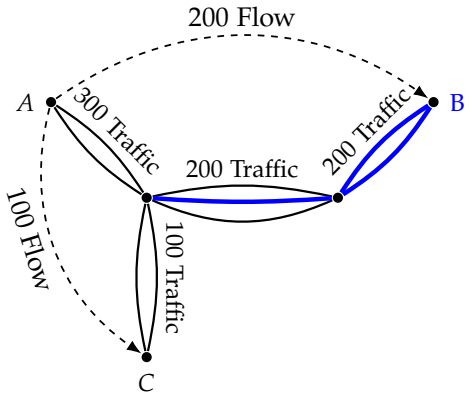
(a) $Dependence^B_A = \frac{1/3 \times 200}{300} \approx 22\%$



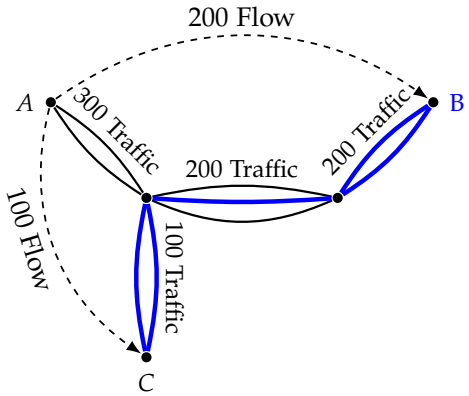
(b) $Dependence^B_C = \frac{0}{100} = 0\%$



(c) $GlobalDependence^B = \frac{200}{300} \approx 67\%$



(d) $GlobalDependence^B = \frac{200+100}{300} = 100\%$



Figures 7c and 7d instead represent global dependence on B for different configurations of B's ownership. We see that global dependence is driven by flows and the geography of ownership. Noticeably, these figures show that global dependence on B would not change if B did not have ownership of the cable in corridor $C2$. The reason is that once B monopolizes the segment closest

to B, then it can already affect (e.g., spy on) 100% of the flows between A and B, thus owning another cable on a corridor that carries the same flow will not increase B's intel nor its ability to pressure A. This idea justifies our focus on the maximum ownership share along the path, rather than other statistics like the mean.

5 Main Results

5.1 Finding 1: Hegemons Dominate (and Weaponize) Telecom Networks

A first central finding of our analysis is that hegemons have historically dominated the global telecommunication infrastructure and have repeatedly used their control for strategic purposes. This pattern spans the entire history of long-distance communication, from the telegraph era to the present-day internet and satellite networks.

Network ownership over time: geopolitics and technology. Figure 8 shows how different countries have contributed to the global expansion of cable and satellite networks over time. In the early years of submarine cables, the United Kingdom led the industry. It benefited from a first-mover advantage and strong access to credit, allowing British firms to build most of the early telegraph network. After WW2, however, British firms could no longer finance new systems at the same pace as they retired old ones. This led to a gradual decline in the UK's global role. During the same period, the United States expanded its network and emerged as the new dominant player.

Figure 9 focuses on the ownership shares of major powers. For cables, the turning point came with the fiber-optic revolution of the 1980s. American firms quickly adopted the new technology and rapidly expanded their networks, securing a dominant position in the global infrastructure. As with cables, the evolution of satellite ownership has been shaped by both geopolitical shifts and technological change. During the Cold War, the Soviet Union was the main player in the satellite segment. This was partly due to its geography: with limited sea access and a location closer to the poles, the Soviet Union had a comparative advantage in satellite-based systems. But after the Cold War, the collapse of the Soviet Union and Russia's economic crisis in the 1990s allowed the United States to compound its leadership in the cables segment with dominance in the

Figure 8: Ownership of telecommunications technology

(a) Ownership of the global submarine cable network

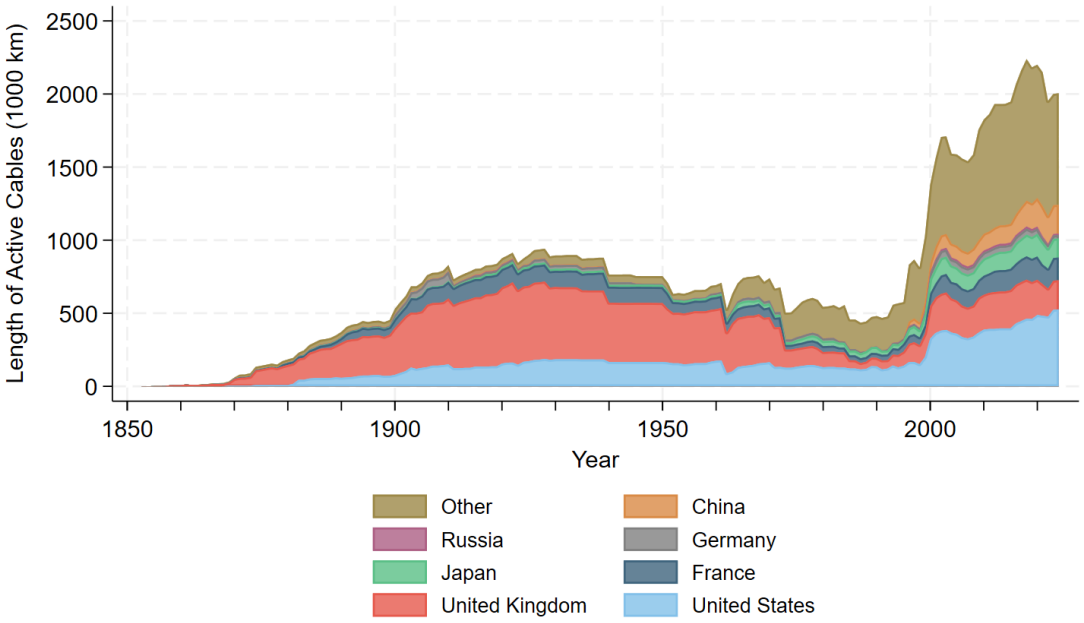
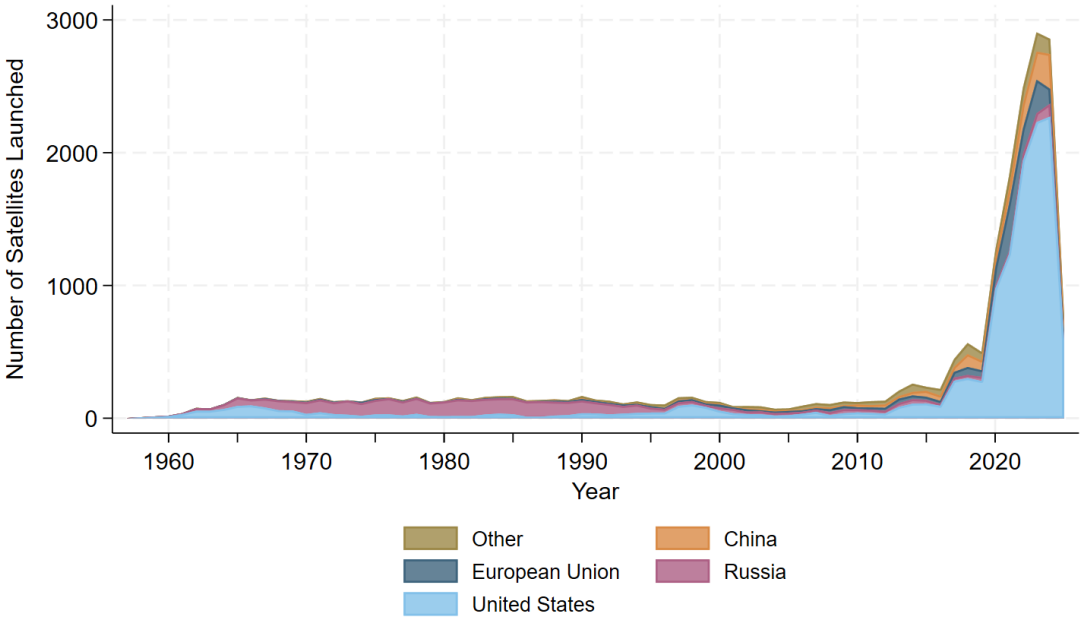


Figure 8: Ownership of telecommunications technology (continued)

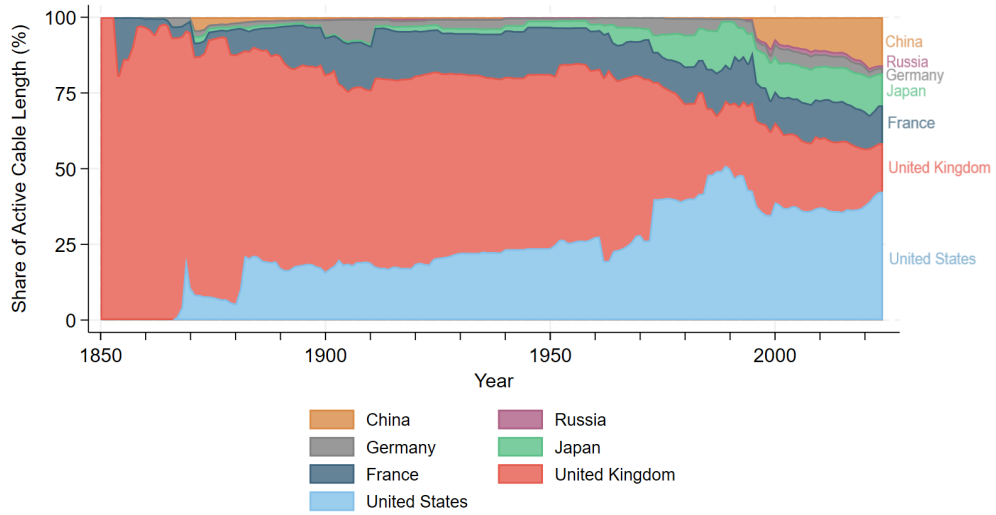
(b) Ownership of the global satellite network



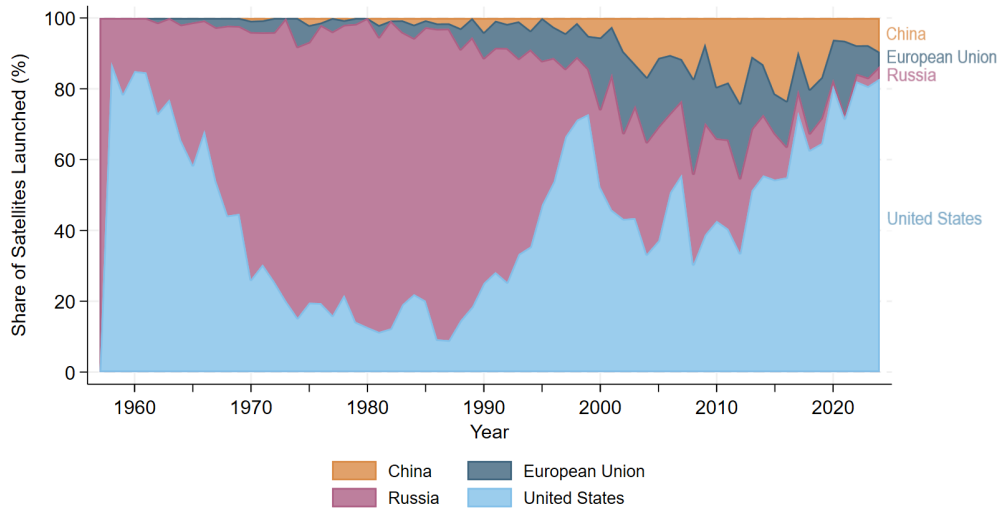
satellites segments. Additionally, American firms strengthened their position again in the 2010s, by developing and rolling out new satellite systems based on technologies such as spot beam architecture and phased array antennas. These advances allowed the US to increase its market share steadily, even as new competitors such as Chinese companies entered the market and Russian as well as European investments began to grow again.

Figure 9: Great powers' ownership of telecommunications technology

(a) Share of the global submarine cable network among great powers



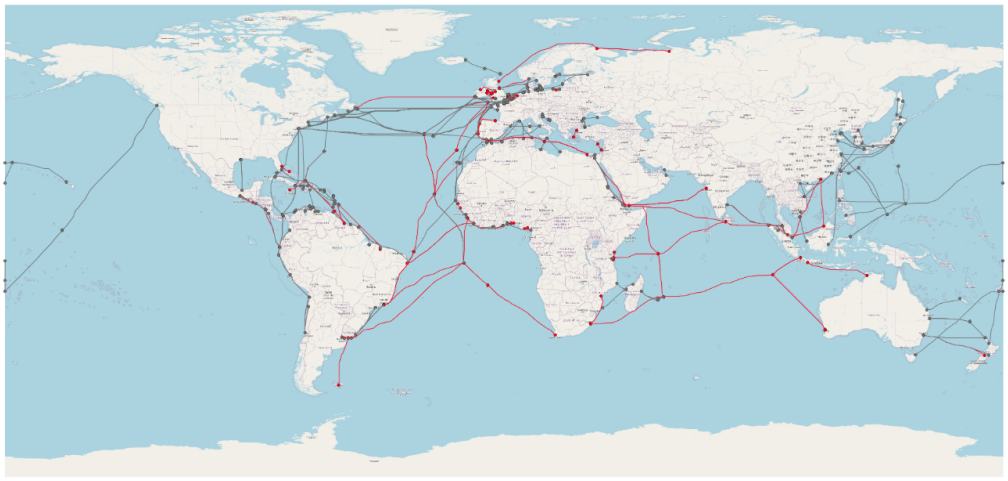
(b) Share of the global satellite network among great powers



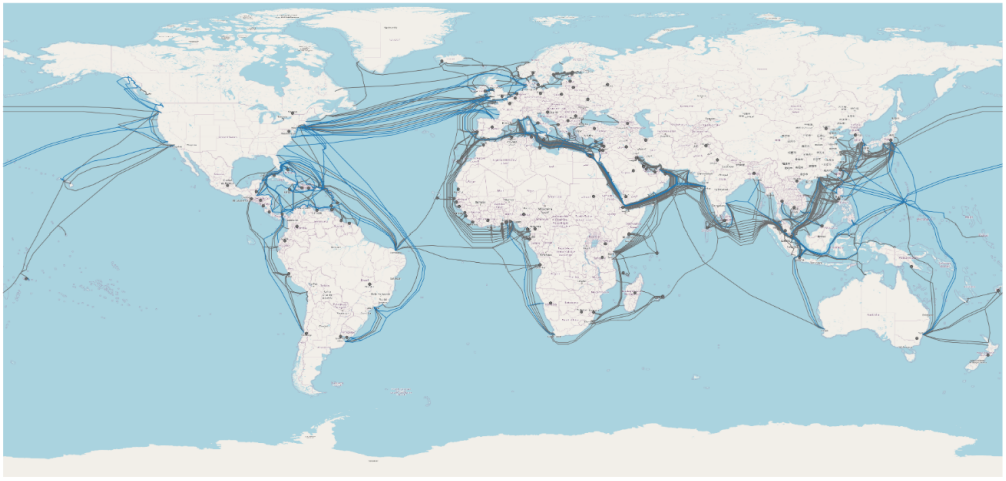
Hegemons as global backbone providers. Figure 10 compares the British-controlled global network in 1930 with the current US-controlled network. Both reveal a defining feature of hegemonic strategy: control over a genuinely global network that extends well beyond the hegemon's own borders or immediate strategic interests. These networks serve not only to connect the hegemon's colonies, allies, or commercial partners, but to offer backbone services to the rest of the world. The widespread geographical reach of these networks translates into espionage capability and leverage. While both the UK and US built expansive networks, the geographic focus of their connectivity strategies differed in ways that reflect their national interests.

Figure 10: Global reach of the hegemon's network: 1930 vs 2024

(a) 1930 Network: UK-controlled cables in red, other cables in gray

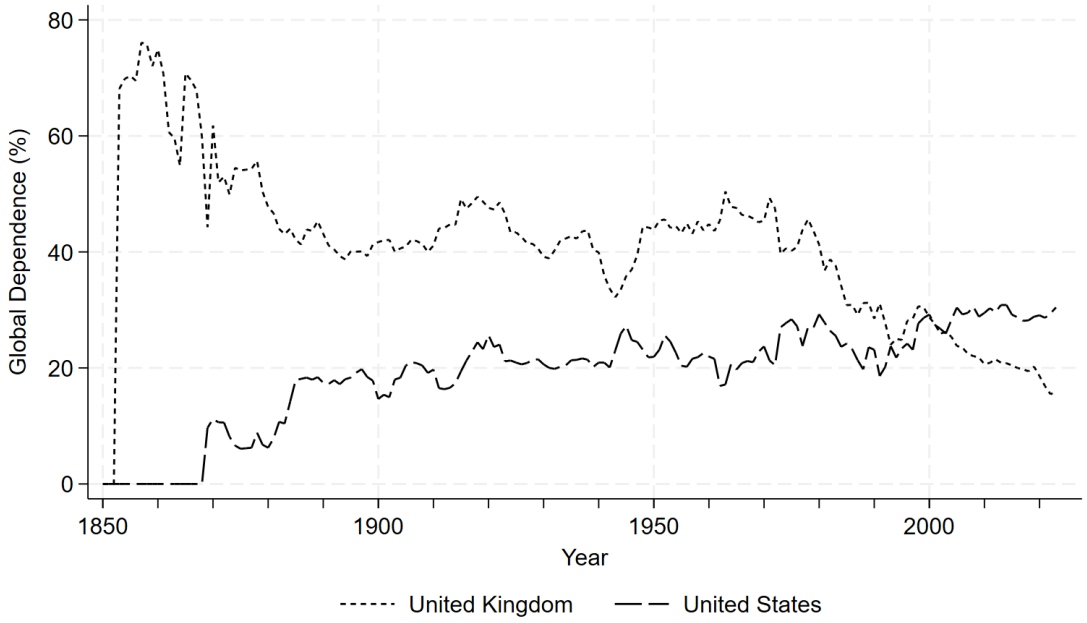


(b) 2024 Network: US-controlled cables in blue, other cables in gray



Hegemonic dominance and weaponization. To conclude, Figure 11 provides a long-run view of global dependence on the United Kingdom and the United States. Recall that dependence on a given country is defined as the share of global telecom flows that is routed on cables owned (at least in part) by entities headquartered in that country. As a result, it is not only driven by the number of cables controlled by a country, but also by their geographic distribution. In line with the previous discussion, we see that for much of the twentieth century, roughly 40% of global flows were routed on British-owned infrastructure. This dominance declined sharply in the 1980's. Despite the presence of many more players in the modern period, the US today controls as much as 30% of global cable-based data flows. This is a testament of US investments in the network and their increasingly central position in the network.

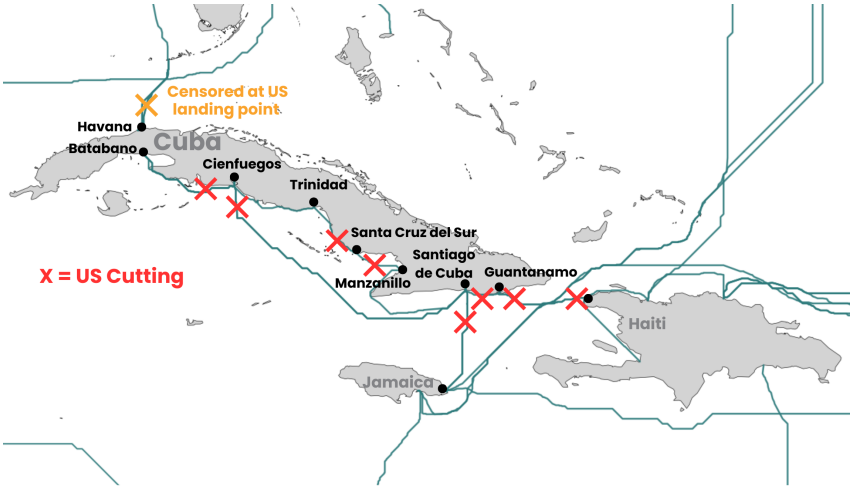
Figure 11: Global dependence of UK and US over time



As discussed in Section 2, both Britain and the United States weaponized this dominance. In 1898, the United States cut or censored cable links between Cuba and Spain, disrupting military communications. A US Navy officer later concluded that "reliable submarine [cable] communications under exclusive control [...] exercise a dominating influence upon the control of the seas" and that it was mostly "coal and cables" that won the war (Winkler, 2008). Figure 12 illustrates this informational blockade for communication around Cuba, showing all telegraph cables as of early 1898. The red crosses mark the affected cables

rather than the precise points of severance. The cable to Florida was censored at the US landing point in Key West.

Figure 12: US cable cutting in the Spanish-American War of 1898



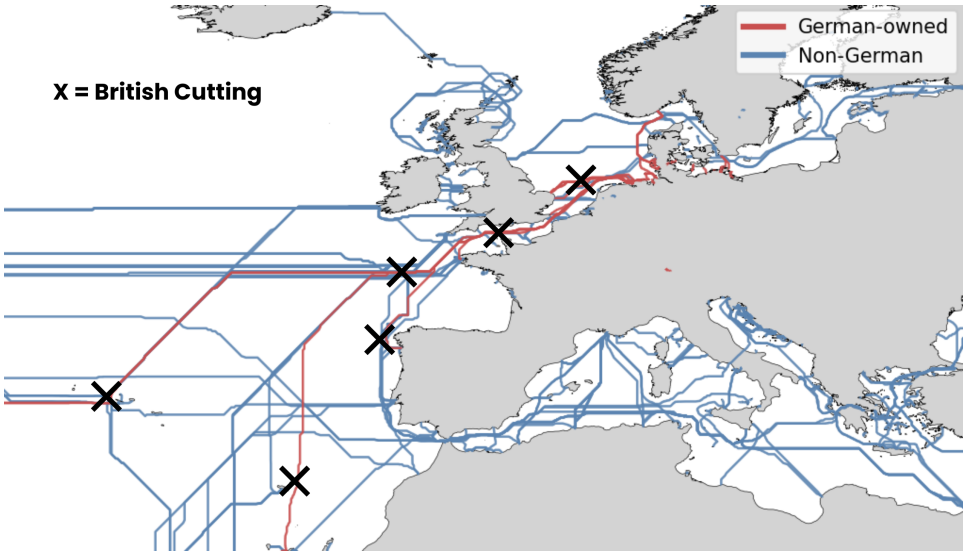
In 1914, Britain severed most of Germany's direct overseas cables and later cut re-routed connections in the Atlantic. Figure 13 displays the telegraph cable network around Germany as of early 1914, with red cables denoting German-owned cables (including state-owned). The black crosses mark the affected cables rather than the precise points of severance. Cables cut by other nations are not included.

These cable cuts isolated Germany from global communications and enabled British espionage, as any telegram had to be sent through enemy cables. The most consequential result was the interception of the Zimmermann Telegram, in which Germany proposed a military alliance with Mexico against the United States. Its decryption and publication in early 1917 led to a public outcry in the US and accelerated the US decision to enter the war against Germany.

These historical episodes underscore the relevance of communications infrastructure as an instrument of coercion which conferred both military and intelligence advantages. There is little reason to expect such leverage to weaken: political willingness in the United States to deploy coercive tools remains substantial, and the close alignment between the state and major technology firms that now finance much of the cable network suggests that future attempts to weaponize the network would likely face limited private-sector resistance.

Overall, the analysis reveals a recurring pattern: hegemonic powers not only control the physical infrastructure of global communications, but also exploit that control for geopolitical advantage. The disruptions surrounding Cuba in 1898

Figure 13: British cable cutting during WW1 (1914-1915)



and during WW1, in particular, triggered substantial investment by secondary powers in alternative and redundant infrastructure to reduce dependence on hegemonic networks and exposure to rival powers. This result motivates the subsequent analysis of investment behavior.

5.2 Finding 2: Geopolitical Risk Spurs Investment in (Redundant) Independent Cable Systems

Our second finding is that geopolitical tensions systematically shape investment in international telecommunications infrastructure. Beyond responding to market incentives, countries and firms build submarine cables as a form of strategic insurance leading to investments in times of high geopolitical risk driven by countries with strained relations with the hegemon.

Economic vs. Geoeconomic Incentives. We think of submarine cable construction as a form of market entry into a corridor-specific transit market. Standard economic reasoning would suggest that the number of active firms in a market (thus in a corridor) should increase with market size (e.g., expected data flows) and decrease with entry costs. However, in a setting where firms or governments seek to reduce dependence on adversarial powers, investment may also be driven by strategic, non-commercial motives. Such strategic motives may reflect in cable-building booms in times of geopolitical risk. To distinguish these motives, we start analyzing the following regression specification at the corridor (m)-year

(t) level:

$$\text{NumActiveFirms}_{mt} = \beta_1 \text{GlobalTraffic}_{mt} + \gamma \text{GeopolRisk}_t + \alpha_m + \text{Controls}_{mt} + \varepsilon_{mt}$$

where $GlobalTraffic_{mt}$ is the log of the variable for Global Traffic that we created in Section 4.2 to measure the expected traffic in a given corridor-year. Instead, $GeopolRisk_t$ is the log of the historical Geopolitical Risk Index (GPR) from Caldara and Iacoviello (2022). Finally, α_m absorbs time-invariant corridor-specific entry costs and $Controls_{mt}$ includes a linear time trend and a measure of globalization ($GlobalTrade/GlobalGDP$). In such specification, a positive γ indicates that investments respond positively to geopolitical tensions, i.e., that we find evidence of geoeconomic entry.

Aggregate-Level Results. Table 1 shows that, as expected, market size has a positive and significant effect on entry. More interestingly, geopolitical risk is also positively associated with the number of active firms, across different risk measures: the continuous GPR index from Caldara and Iacoviello (2022), an indicator for high-risk periods (years with above average GPR index), and a forward-looking "High War Risk" indicator that is $= 1$ in the decade that preceded major great power wars.

Country-Level Specification. To dig deeper, we disaggregate the data and estimate regressions at the country (j)-corridor (m)-year (t) level. This enables to see whether the relation between investments and geopolitical risk resists to a specification that better characterizes economic incentives and includes conditioning variables at the country-year level. The baseline specification is:

$$\begin{aligned}\text{NumActiveFirms}_{jmt} = \beta_1 \text{GlobalTraffic}_{mt} + \beta_2 \text{DomesticTraffic}_{jmt} \\ + \gamma_1 \text{GeopolRisk}_t + \alpha_{jm} + \text{Controls}_{jmt} + \varepsilon_{jmt}\end{aligned}$$

First, note that the specification now includes the variable $\text{DomesticTraffic}_{jmt}$ which is the log of the share of j domestic traffic divided by global traffic. This variable captures how much of the market's total traffic originates or ends in country j, effectively measuring how "relevant" the corridor is to that country. While this variable could be interpreted in terms of geopolitical incentives, it could also reflect economic motivations. For example, we could expect firms from a given country to be more attracted from investing on corridors with high domestic data flows, as they are better informed about the prospects of such

Table 1: Effect of Global Geopolitical Risk on Corridor-Level Investment

	(1)	(2)	(3)
	$NumActiveFirms_{mt}$		
Global Traffic	0.05***	0.05***	0.07***
	[0.016]	[0.016]	[0.015]
Geopolitical Risk Index (GPR)	0.06***		
	[0.020]		
High GPR (above avg.)		0.08***	
		[0.030]	
High War Risk			0.16***
			[0.036]
Market FE	Yes	Yes	Yes
Observations	2,008	2,008	2,458

Notes: Dependent variable: number of active firms in corridor m and year t. "Global Traffic" is the log of our estimate of all traffic flows routed in corridor m in year t based on trade flows and our traffic assignment algorithm. GPR is the geopolitical risk index of Caldara and Iacoviello (2022). High GPR (above avg.) is an indicator which is $= 1$ when the GPR index is above average and 0 otherwise. High War Risk is based on the share of major cable-owning countries expected to be involved in war within 15 years. All columns condition o linear time trends and global trade openness ($GlobalTrade/GlobalGDP$). Robust standard errors in brackets. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

corridors. With this interpretation, a large coefficient on $DomesticTraffic$ would indicate that this informational effect is large. Additionally, this specification allows us to include α_{jm} which is a country-corridor fixed effect capturing time-invariant country-corridor specific differences in entry costs or benefits. Note that this fixed effect is much more stringent than simply including α_m and α_j, so we are still capturing corridor-level fixed effect, as well as any time-invariant country-level characteristic (e.g., geography) that might lead a country to be more or less likely to invest in submarine cables. Finally, in this specification we enrich the set of controls by adding country-year controls. Specifically, we include the log of GDP_{jt} and Pop_{jt}, country j's $GDPpc_{jt}$, and its openness to trade $Trade_{jt}/GDP_{jt}$.

Country-Level Results. Table 2 shows that both $GlobalTraffic$ and $DomesticTraffic$ are significant predictors of firm entry. Crucially, the coefficient on $GeopolRisk$ remains positive and significant even after controlling for these economic incentives and adding rich fixed effects. This confirms that geopolitical tensions have an independent effect on investment decisions.

Which countries engage in geopolitical investments? As a final step, we study the differential investment strategies of the countries involved. We do this along two dimensions: we study whether certain countries are relatively more likely to invest (1) in times of geopolitical risk (2) and in regions where their domestic interests are greater. Specifically, we study the potentially heterogeneous behavior of the following types of countries: the hegemon (defined as the UK before 1950 and the US afterwards) and countries with a strained relation with the hegemon. To test these hypotheses, we augment the model with interaction terms that capture the heterogeneity we are interested in. Starting from the hegemon, we estimate the following equation:

$$\begin{aligned}\text{NumActiveFirms}_{jmt} = {} & \beta_1 \text{GlobalTraffic}_{mt} + \beta_2 \text{DomesticTraffic}_{jmt} + \\ & + \beta_3 \text{DomesticTraffic}_{jmt} \cdot \mathbf{1}\{j = Hegemon_t\} + \\ & + \gamma_1 \text{GeopolRisk}_t + \\ & + \gamma_2 \text{GeopolRisk}_t \cdot \mathbf{1}\{j = Hegemon_t\} + \\ & + \alpha \mathbf{1}\{j = Hegemon_t\} + \alpha_{jm} + \text{Controls}_{jmt} + \varepsilon_{jmt}\end{aligned}$$

Instead, we measure the extent to which countries have a strained relation with the hegemon based on the value of the country-hegemon foreign policy similarity

Table 2: Effect of Geopolitical Risk on Country-Corridor Investments

	$NumActiveFirms_{jmt}$				
	(1)	(2)	(3)	(4)	(5)
Domestic Traffic	1.40***	1.40***	1.28***	1.23***	3.44***
	[0.517]	[0.485]	[0.365]	[0.403]	[0.466]
Global Traffic	0.13**	0.11**	0.10***	0.16***	0.37**
	[0.054]	[0.051]	[0.034]	[0.061]	[0.165]
Geopolitical Risk Index (GPR)	0.15**				
	[0.063]				
High GPR (above avg.)		0.16***			
		[0.048]			
High War Risk			0.23***		
			[0.069]		
Market-Country FE	Yes	Yes	Yes	Yes	Yes
Controls	Yes	Yes	Yes	Yes	Yes
Year FE	No	No	No	Yes	Yes
Observations	10,162	10,162	12,232	10,162	19,770

Notes: Dependent variable: number of active firms from country j in corridor m and year t. "Global Traffic" is the log of our estimate of all traffic flows routed in corridor m in year t based on trade flows and our traffic assignment algorithm. "Domestic Traffic" is the log of the share of predicted corridor-level traffic originating from or destined to country j. Both traffic measures are based on global trade flows and our traffic assignment algorithm. GPR is the geopolitical risk index of Caldara and Iacoviello (2022). High GPR (above avg.) is an indicator which is $= 1$ when the GPR index is above average and 0 otherwise. High War Risk is based on the share of major cable-owning countries expected to be involved in war within 15 years. All columns include GDP, population, GDP per capita, and trade openness as controls. Standard errors clustered at country-level in brackets. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

index of the Correlates of War project ($FPSim_{jmt}^{Hegemon_t}$). Specifically, we let $BadRelations_{jmt} = 1 - FPSim_{jmt}^{Hegemon_t}$ and we consider the following estimating equation:[15]

$$\begin{aligned}\text{NumActiveFirms}_{jmt} = {} & \beta_1 \text{GlobalTraffic}_{mt} + \beta_2 \text{DomesticTraffic}_{jmt} + \\ & + \beta_3 \text{DomesticTraffic}_{jmt} \cdot BadRelations_{jmt} + \\ & + \gamma_1 \text{GeopolRisk}_t + \\ & + \gamma_2 \text{GeopolRisk}_t \cdot BadRelations_{jmt} + \\ & + \alpha BadRelations_{jmt} + \alpha_{jm} + \text{Controls}_{jmt} + \varepsilon_{jmt}\end{aligned}$$

Country-level Heterogeneity Results. Tables 3 and 4 report the results of these heterogeneity exercises. A first finding from Table 3 is that the hegemon is significantly more likely to invest than other countries. Note that these specifications include α_{jm} fixed effects, implying that this effect is driven by comparing the investment patterns of the UK and the US in the years in which they were the hegemon relative to the years in which they were not. Moreover, we see that, relative to other countries, the hegemon is less likely to invest in places that serve its national interest. Both these findings are in line with the previous section, where we showed that hegemons build their networks at a much faster rate than others and they end up controlling a world-spanning network. Third, the results do not seem to indicate that the hegemon invests more in times of greater geopolitical risk (if anything, the results suggest that it invests less). Moving to Table 4, we see instead that when a country's relation with the hegemon deteriorates, then it becomes significantly more likely to invest in regions that serve its national interests and it is more likely to invest in times of greater geopolitical risk. Interestingly, the relation between investments and geopolitical risk turns insignificant once we include this interaction, suggesting that such relation is driven by the behavior of countries with bad relations with the hegemon. Finally, note that a worsening relation with the hegemon reduces a country's investment in the network.

Interpretation. Our analysis shows the crucial role of international tensions in affecting the timing and location of cable investments. These findings are consistent with the idea that, in times of geopolitical tensions, countries invest in

[15] Results are robust to focusing on an indicator function which is $= 1$ when $FPSim_{jmt}^{Hegemon_t}$ is below average and $= 0$ otherwise.

Table 3: Differential investment behavior: Hegemon

	(1)	(2)	(3)	(4)	(5)	(6)
			$NumActiveFirms_{jmt}$			
Hegemon × Domestic Traffic	-1.44**	-1.47**	-1.87***	-1.03	-1.10	-1.36**
	[0.723]	[0.674]	[0.461]	[0.732]	[0.716]	[0.576]
Hegemon × GPR	-0.34**			-0.33***		
	[0.170]			[0.108]		
Hegemon × High GPR		-0.21			-0.22	
		[0.230]			[0.167]	
Hegemon × High War Risk			-0.23*			-0.13
			[0.125]			[0.096]
Hegemon (indicator)	2.12***	0.80***	1.22***	1.84***	0.58	0.87***
	[0.593]	[0.265]	[0.175]	[0.407]	[0.358]	[0.293]
Domestic Traffic	1.73***	1.74***	1.72***	1.50***	1.50***	1.56***
	[0.513]	[0.440]	[0.328]	[0.373]	[0.282]	[0.319]
Global Traffic	0.11*	0.09*	0.08*	0.15**	0.14**	0.13***
	[0.061]	[0.057]	[0.047]	[0.065]	[0.065]	[0.040]
Geopolitical Risk Index (GPR)	0.30***					
	[0.050]					
High GPR (above avg.)		0.22***				
		[0.064]				
High War Risk			0.28***			
			[0.086]			
Market-Country FE	Yes	Yes	Yes	Yes	Yes	Yes
Controls	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	No	No	No	Yes	Yes	Yes
Observations	10,162	10,162	12,232	10,162	10,162	12,232

Notes: Dependent variable: number of active firms from country j in corridor m and year t. "Hegemon" is a dummy equal to 1 for the hegemon (UK pre-1950, US post-1950). "Global Traffic" is the log of our estimate of all traffic flows routed in corridor m in year t based on trade flows and our traffic assignment algorithm. "Domestic Traffic" is the log of the share of predicted corridor-level traffic originating from or destined to country j. Both traffic measures are based on global trade flows and our traffic assignment algorithm. GPR is the geopolitical risk index of Caldara and Iacoviello (2022). High GPR (above avg.) is an indicator which is $= 1$ when the GPR index is above average and 0 otherwise. High War Risk is based on the share of major cable-owning countries expected to be involved in war within 15 years. All specifications include GDP, population, GDP per capita, trade openness, and linear time trends as controls. Standard errors clustered at the country-market level. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

Table 4: Differential Investment Behavior: Bad Relations with the Hegemon

	(1)	(2)	(3)	(4)	(5)	(6)
	Active Cables (country *j*)					
Bad Relation × Domestic Traffic	1.16**	1.14***	1.20***	0.96**	0.93**	1.06***
	[0.565]	[0.406]	[0.353]	[0.395]	[0.364]	[0.398]
Bad Relation × GPR	0.46***			0.53***		
	[0.078]			[0.117]		
Bad Relation × High GPR		0.49**			0.71**	
		[0.237]			[0.283]	
Bad Relation × High War Risk			0.21**			0.19**
			[0.091]			[0.095]
Bad Relation (with Hegemon)	-2.17***	-0.37**	-0.42***	-2.35***	-0.31	-0.36**
	[0.415]	[0.176]	[0.118]	[0.543]	[0.214]	[0.164]
Domestic Traffic	0.41	0.38	0.50	0.52	0.51	0.58**
	[0.584]	[0.555]	[0.315]	[0.489]	[0.496]	[0.277]
Global Traffic	0.04	0.03	0.01	0.04	0.04	0.03
	[0.060]	[0.056]	[0.039]	[0.063]	[0.058]	[0.038]
Geopolitical Risk Index (GPR)	-0.10*					
	[0.054]					
High GPR (above avg.)		-0.13				
		[0.091]				
High War Risk			0.00			
			[0.032]			
Market-Country FE	Yes	Yes	Yes	Yes	Yes	Yes
Controls	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	No	No	No	Yes	Yes	Yes
Observations	10,127	10,127	12,197	10,127	10,127	12,197

Notes: Dependent variable: number of active cables involving firms from country j in corridor m and year t. "Bad Relation" measures the foreign policy distance from the hegemon (UK before 1950, US after) using the foreign policy similarity index from the Correlates of War project. "Global Traffic" is the log of our estimate of all traffic flows routed in corridor m in year t based on trade flows and our traffic assignment algorithm. "Domestic Traffic" is the log of the share of predicted corridor-level traffic originating from or destined to country j. Both traffic measures are based on global trade flows and our traffic assignment algorithm. GPR is the geopolitical risk index of Caldara and Iacoviello (2022). High GPR (above avg.) is an indicator which is $= 1$ when the GPR index is above average and 0 otherwise. High War Risk is based on the share of major cable-owning countries expected to be involved in war within 15 years. All specifications include GDP, population, GDP per capita, trade openness, and linear time trends as controls. Standard errors clustered at the country-corridor level. * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

reducing their dependence on the hegemon, building parallel global networks. While such investments may appear wasteful from an economic perspective, countries might find that they provide valuable insurance against the risks of coercion.

5.3 Finding 3: Global Data Flows Are Highly Vulnerable to Disruptions

Our third finding highlights the vulnerability of global data flows to both accidental and deliberate disruptions. This vulnerability arises from the concentration of flows on a limited number of corridors with limited cable redundancy. Our vulnerability metric provides a clear framework to identify risks that may not be immediately visible from aggregate infrastructure data. It offers a diagnostic tool for policymakers to assess where additional investment in redundancy is most urgently needed. This framework can be flexibly applied at the level of countries, corridors, or individual strategic chokepoints to support proactive infrastructure planning.

Sources of Disruption. Submarine cables are susceptible to a range of natural and man-made hazards. Geological events such as undersea earthquakes, volcanic activity, and landslides can sever cables unexpectedly. In addition, incidents such as anchor drags from fishing vessels or accidental damage from maritime activity can result in partial or full disruptions. Though repairs are often completed within days or weeks, the downtime can cause substantial communication blackouts in the affected regions. Such risk becomes more severe in the context of deliberate sabotage or military conflict. One reason is that such events may affect multiple cables simultaneously; another reason is that cable-repairs might be impossible in active conflict zone.[16]

Identifying Vulnerable Corridors. Table 5 shows the top ten submarine corridors by global vulnerability.[17] The most vulnerable corridor is intra–East Asia, which handles 28.4% of global data flows but is served by only 14 cables, implying that each cable carries approximately 2% of global traffic. By contrast, the South China Sea corridor, though critical, has a larger number of cables (35) and thus lower per-cable vulnerability (0.7%). Still, a coordinated attack that disables

[16] In Section 2 we discuss several episodes of cable cutting in times of war.

[17] Recall that global vulnerability is the share of global telecom flows routed on each cable in a given corridor.

half of those cables would affect more than 10% of global data flows. Another surprising vulnerability lies in the northern Indian Ocean corridor, where limited infrastructure means each cable carries more than 1.6% of global traffic.

Table 5: Top 10 submarine corridors by global vulnerability

	# of Cables	% of Global Data	% of Global Data per Cable
Asia East (intra)	14	28.4	2.0
Europe South (intra)	39	25.5	0.7
Asia Southeast (intra)	35	23.4	0.7
Europe North (intra)	24	22.0	0.9
Asia Southwest (intra)	24	19.1	0.8
Pacific W - NW	33	15.4	0.5
Indian Ocean N - E	8	13.1	1.6
Atlantic NW - NE	19	8.9	0.5
Pacific NW - NE	17	8.2	0.5
America Caribbean (intra)	24	3.5	0.1

Country-Level Vulnerability. To gain a better insight into the drivers of global vulnerabilities, we can look at Table 6 which reports the three most vulnerable submarine corridors for each major economy. One thing that is immediately noticeable is that the trans-Indian vulnerability is much smaller for the USA than any other country. This can explain why the trans-Indian corridor is emerging as a global chokepoint: while it is important globally, the main investor in cables (the USA) has little interests in the region. Looking at the other parts of the Table, we can see that China and Japan both display an above average exposure to the intra–East Asian and Indian Ocean corridors. China's smaller exposure to intra-Asia than Japan is due to China's ability to exchange data with its neighbors using terrestrial corridors. Similarly, terrestrial networks are a major reason why Germany and France have significant less exposures than the UK. Indeed, while France and Germany can count on the intra-European terrestrial network, Britain has to route all its data flows on submarine corridors. Finally, the US shows a remarkably balanced portfolio of exposures, with equal vulnerabilities to East Asia, the trans-Atlantic and the trans-Pacific.

Europe's key vulnerability: the North Sea corridor. Table 7 illustrates the top 8 countries by vulnerability to the Northern European corridor, showing that the UK as well as Scandinavian countries like Norway, Sweden are particularly exposed to disruptions in the North Sea region. Given that the Norther European corridor consists of only 24 cables, we see that a coordinated sabotage to half of

Table 6: Top 3 submarine vulnerabilities for each major economy

	Markets with Highest Vulnerability per Country (% / #)		
	Top 1	Top 2	Top 3
China	Asia East (6.1 / 14)	trans-Indian (3.5 / 8)	Pacific SE-NE (3.0 / 2)
Japan	Asia East (7.1 / 14)	trans-Indian (3.0 / 8)	Pacific NW-NE (1.3 / 17)
UK	Europe North (3.0 / 24)	trans-Indian (2.0 / 8)	Asia Southwest (0.9 / 24)
France	Europe North (1.3 / 24)	trans-Indian (1.2 / 8)	Europe South (0.6 / 39)
Germany	Europe North (1.7 / 24)	trans-Indian (1.5 / 8)	Europe South (0.8 / 39)
USA	Atlantic NW-NE (1.6 / 19)	Asia East (1.5 / 14)	Pacific NW-NE (1.3 / 17)

the cables in the region would affect more than 20% of the data flows of each of the reported countries.

Table 7: Top 8 country by vulnerability to the Northern European corridor

	Vulnerability
Norway	3.2
Sweden	3.0
UK	3.0
Denmark	2.9
Netherlands	1.7
Germany	1.7
Portugal	1.7
Russia	1.7

Strategic Implications. These findings suggest that resilience to telecom disruption is not evenly distributed. Some regions and countries remain dangerously exposed, while others have invested heavily in redundancy and diversification. Historical precedent shows that powerful countries have responded to such vulnerabilities with big and coordinates investments. The British "All Red Line" was built so that every cable would only land in a port that fell under British control. This ensured cable security near shorelines, where attacks were most likely. The modern analogue is perhaps the United States' investments into making Guam a central data hub in South East Asia. However, in the contemporary setting, physical protection alone is insufficient. Given the technological feasibility of deep-sea cable cutting, the most viable insurance policy is redundancy: investing in a sufficient number of geographically diverse routes to increase the cost and complexity (and decrease the value) of any sabotage attempt. As we have seen, the United States seems to have already engaged in those type of investments. Certainly, Europe has benefited from such investments in key corridors such as South East Asia and trans-Atlantic. However, as exemplified by the vulnerability

in the Indian Ocean and in the North Sea, European and American incentives are not sufficiently align to rely solely on American investments.

6 Preview: cable-level results on dependence and vulnerability

This section presents preliminary cable-level results for 2023 from ongoing work that extends our traffic assignment framework from corridors to individual cables and cable segments. In practice, we start from the same bilateral flow matrix and shortest-path logic introduced in Section 4, but we move from a corridor-based representation of the network to the cable systems and segments that implement those connections. We then combine these cable-level paths with ownership information to recover more granular measures of dependence and vulnerability. More specifically, the cable-level exercise traces which exact systems and segments lie on the assigned route and links them to cable-specific ownership rather than treating the corridor as a single homogeneous conduit. At the cable level, the assignment is also sensitive to capacity and congestion, which helps generate a more realistic allocation of traffic across alternative routes. This makes it possible to distinguish between broad corridor exposure and exposure concentrated on particular cable systems, landing-point approaches, or ownership structures. The purpose of this exercise is to provide a preview of results once the analysis moves from corridors to cables.

6.1 Dependence on US and Chinese cable infrastructure

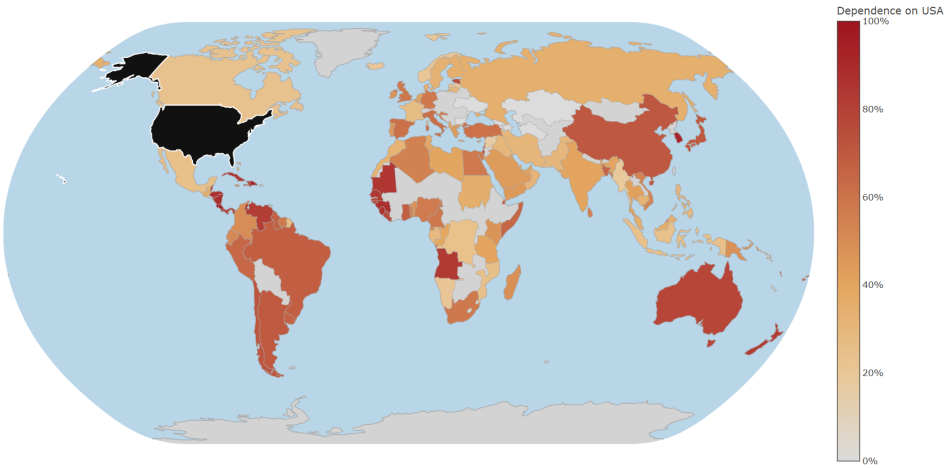
The dependence maps translate hegemonic control from corridor space into cable space. A country is dependent on US or Chinese infrastructure when a large share of its traffic is routed on cables owned or co-owned by entities from that country. Figure 14 shows that dependence on US-controlled infrastructure remains strikingly broad and global in 2023. High dependence is visible not only in the Western Hemisphere, but also across East Asia, Oceania, and parts of Europe, Africa, and the Middle East. This pattern reinforces our earlier finding that the United States acts as a global backbone provider whose cable footprint extends well beyond its own geography.

The China map reveals a different but still consequential pattern. Dependence on Chinese-controlled infrastructure is more regionally concentrated, with especially strong exposure across East and Southeast Asia and along parts of

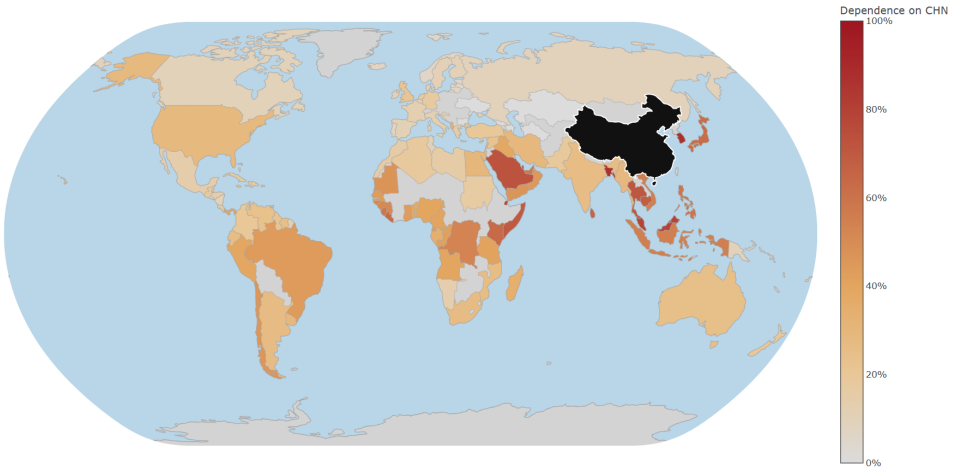
the Indian Ocean, the Gulf, and the Red Sea corridor. Relative to the United States, Chinese cable influence is less uniformly global, but in its core theaters it is already substantial. In this sense, the cable-level perspective preserves the paper's main argument about hegemonic control while revealing more clearly where rival infrastructures matter most in practice.

Figure 14: Dependence on US and Chinese infrastructure in 2023

(a) Dependence on US cables, 2023



(b) Dependence on Chinese cables, 2023



Note: These maps visualize country-level dependence on subsea cable infrastructure of a) the US and b) China. Darker shades indicate that a larger share of a country's traffic is routed on cables owned or co-owned by entities from the focal country. The focal country itself is shown in black.

6.2 Cable-level vulnerability

Vulnerability at the cable level captures a different dimension of exposure. Instead of asking who owns the infrastructure, it asks which specific cables and

cable segments carry a country's traffic and therefore constitute points of concentrated disruption risk. The resulting maps show that the aggregate corridor vulnerabilities documented in Section 5.3 are often driven by a surprisingly small number of identifiable segments.

East Asia stands out. Figure 15 displays the vulnerability of Japan, China, and India to specific cables, respectively. Japan shows a high concentration of traffic on a limited number of links connecting to Korea, Taiwan, and the Pacific, indicating that disruptions to a small set of cables could have outsized consequences. China's map reveals a similarly concentrated risk structure, with prominent vulnerable segments in the South China Sea and in the links connecting China to Korea and Japan. In both cases, the cable-level perspective makes visible how regional concentration and geopolitical sensitivity overlap.

India's map highlights a different but equally important chokepoint structure. The most exposed segments run westward through the Arabian Sea toward the Gulf and onward toward Suez, underscoring India's reliance on a narrow set of cable routes linking South Asia to Europe and the Middle East. This is a cable-level counterpart to the Indian Ocean vulnerability emphasized in Section 5.3, but with a more precise geographic focus on the Hormuz-Suez axis.

Taken together, these maps suggest that the cable-level approach is especially useful for identifying the precise segments where redundancy remains limited and where disruptions would be especially costly.

Figure 15: Cable-level vulnerability of selected economies in 2023

(a) Japan

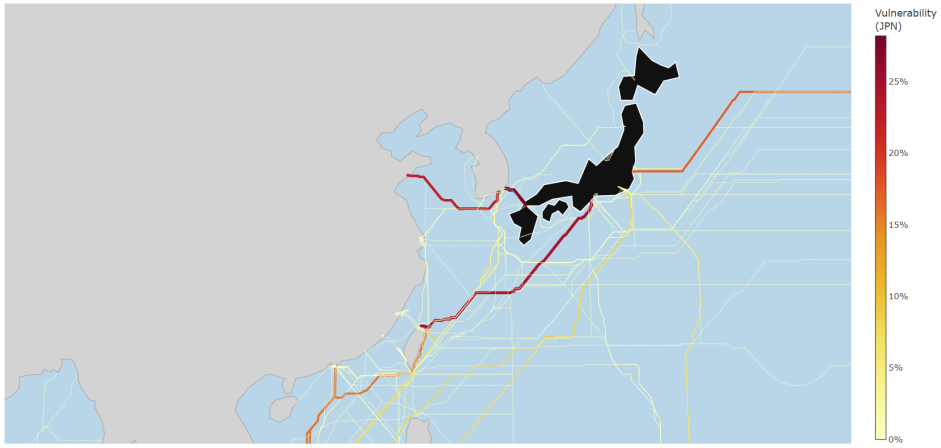
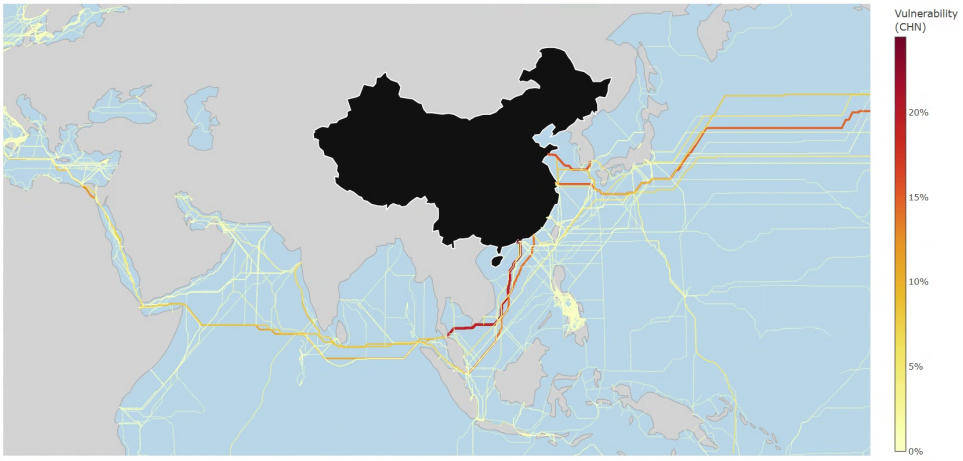
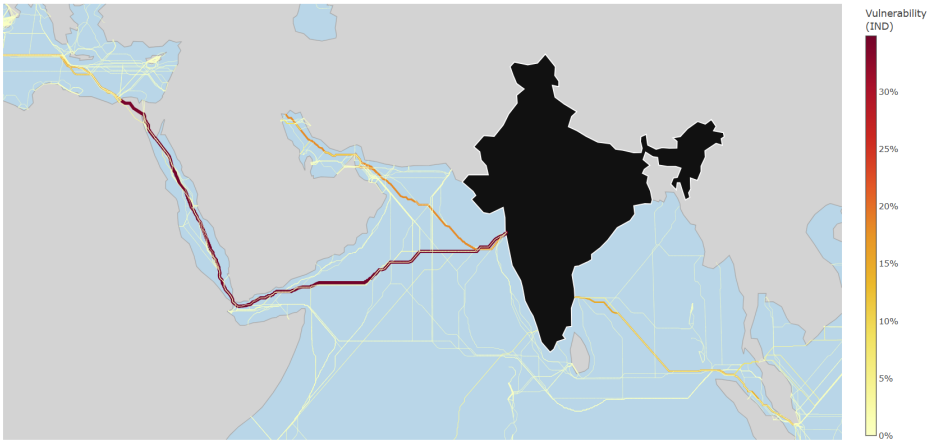


Figure 15: Cable-level vulnerability of selected economies in 2023 (continued)

(b) China



(c) India



Note: These maps visualize cable-level dependence on the subsea cable infrastructure connecting a) Japan, b) China, and c) India with global traffic. Darker segments indicate that a larger share of the focal country's traffic traverses that cable segment. The focal country is shown in black.

7 Conclusion

Telecommunication infrastructure is the backbone of the global economy. This paper presents the *CableHist* database, the first granular, long-run dataset on global telecommunication networks, from the first telegraph line across the Channel to the latest Starlink satellite launches.

Using the *CableHist* data and a traffic assignment model adapted from network economics, we propose an empirical framework that systematically quantifies each country's exposure to cable-related geopolitical risks such as embargoes or sanctions (dependence) and sabotage (vulnerability), identifying chokepoints

and exposures.

We then use the traffic assignment model to disentangle economic and geopolitical motives in cable-building. This exercise demonstrates the crucial role of geopolitical tensions in shaping investments in the network and, consequently, its evolution. First, we show that hegemonic dominance over telecom infrastructure is a historical constant. The global hegemon (first the UK, now the US) has maintained a cable network extending well beyond its immediate vicinity and strategic interests, and both have weaponized these networks to coerce other countries. Second, we show that geopolitical risk spurs investment. Specifically, we find that, in times of geopolitical tension, countries with strained relations with the hegemon increasingly invest in their own networks in ways that cannot be explained by changes in the expected profitability of such cables. This pattern is evident historically (e.g., France and Germany before WW1) and in the present (e.g., China since 2000). Third, despite such geopolitically motivated investments, the global network remains highly vulnerable to sabotage and conflict. A small number of cable cuts could generate major disruptions, especially in regions like East Asia, Northern Europe, and the Indian Ocean.

Taken together, our findings imply that the political economy of global telecommunications is characterized by recurring tensions between security and efficiency. In peaceful times, the system tends to consolidate around hegemonic infrastructure; in periods of rising rivalry, countries seek to hedge and decouple from the hegemon. As global tensions rise and the digital economy expands, the geoeconomics of submarine cables will only become more central. Our study offers a historical lens and a quantitative framework to better understand and ultimately mitigate the risks embedded in the vital yet invisible infrastructure.

References

Ahvenainen, Jorma, *The Far Eastern Telegraphs: the History of Telegraphic Communications between the Far East, Europe, and America before the First World War*, Helsinki: Suomalainen Tiedeakatemia, 1981.

__ , *The History of the Caribbean Telegraphs before the First World War*, Helsinki: Suomalainen Tiedeakatemia, 1996.

__ , *The European Cable Companies in South America: Before the First World War*, Helsinki: Academia Scientiarum Fennica : Distributed by Tiedekirja, 2004. OCLC: ocm54512593.

__ , *The History of the Near Eastern Telegraphs before the First World War*, Helsinki: Finnish Academy of Science and Letters, 2011. OCLC: ocn733408869.

Aldrich, Richard J., *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*, London: HarperCollins Publishers, 2011.

Allen, James, "*Report of Col. James Allen, Chief Signal Officer, Army of Porto Rico, of the Operations of the Signal Corps on the South Coast of Cuba and in Porto Rico*," 1898.

Allen, Treb and Costas Arkolakis, "Trade and the Topography of the Spatial Economy," *Quarterly Journal of Economics*, August 2014, *129* (3), 1085–1140.

__ **and** __ , "The Welfare Effects of Transportation Infrastructure Improvements," *The Review of Economic Studies*, 2022, *89* (6), 2911–2957.

__ **and** __ , "Quantitative Regional Economics," January 2025.

Andrew, Christopher, *The Defence of the Realm: The Authorized History of MI5*, London New York, New York Toronto Dublin Camberwell New Delhi Rosedale, Auckland Johannesburg: Penguin, 2010.

Arkolakis, Costas and Conor Walsh, "Clean Growth," NBER Working Paper 31615 2023.

Bamford, James, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, New York: Anchor Books, 2002.

Bertsch, Gary K., ed., *Controlling East-West Trade and Technology Transfer: Power, Politics, and Policies*, Durham, NC: Duke University Press Books, 1988.

Bragadin, Marc' Antonio, *The Italian Navy in World War II*, Naval Institute Press, 1957.

Bruton, Elizabeth, "The Cable Wars: Military and State Surveillance of the British Telegraph Cable Network During World War One," *Marklund, Andreas and Mogens Rüdiger (ed.s). Historicizing Infrastructure (Aalborg: Aalborg University Press, 2017)*, January 2017.

Caldara, Dario and Matteo Iacoviello, "Measuring Geopolitical Risk," *American Economic Review*, April 2022, *112* (4), 1194–1225.

Caoui, El Hadi and Andrew Steck, "Diversification, Market Entry, and the Global Internet Backbone," *Review of Economic Studies*, 2025. Advance article.

Clayton, Christopher, Antonio Coppola, Matteo Maggiori, and Jesse Schreger, "Geoeconomic Pressure," 2025. NBER Working Paper No. 34020.

__ **, Matteo Maggiori, and Jesse Schreger**, "Putting Economics Back into Geoeconomics," in John V. Leahy and Valerie A. Ramey, eds., *NBER Macroeconomics Annual 2025, Volume 40*, Macroeconomics Annual, University of Chicago Press, 2025, chapter 2.

__ **,** __ **, and** __ , "A Framework for Geoeconomics," *Econometrica*, 2026, *94* (1), 105–136.

Conley, Heather A., Sophie Arts, Kristine Berzina, and Frida Rintakumpu, "*Protecting Undersea Infrastructure in the North American Arctic: Lessons from Incidents in the Baltic Sea and High North*," May 2024.

Craven, John P., *The Silent War: The Cold War Battle Beneath the Sea*, 1st touchstone ed ed., New York, NY: Touchstone, 2002. OCLC: 49503087.

Department of Veterans' Affairs, *Snapshots: Australians in War and Conflict*, Canberra: Department of Veterans' Affairs, September 2024.

Donaldson, Dave, "Railroads of the Raj: Estimating the Impact of Transportation Infrastructure," *American Economic Review*, April 2018, *108* (4-5), 899–934.

Fajgelbaum, Pablo D. and Edouard Schaal, "Optimal Transport Networks in Spatial Equilibrium," *Econometrica*, 2020, *88* (4), 1411–1452.

Farrell, Henry and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security*, 2019, *44* (1), 42–79.

__ **and Abraham Newman**, *Underground Empire: How America Weaponized the World Economy*, London: Allen Lane, 2023.

Fishman, Edward, *Chokepoints: American Power in the Age of Economic Warfare*, New York: Portfolio/Penguin, 2025.

Gallea, Quentin, Massimo Morelli, and Dominic Rohner, "Power in the Pipeline," mimeo October 2022.

Giles, Keir, "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power | Chatham House – International Affairs Think Tank," 2016.

Goodrich, Caspar F., "*The St. Louis' Cable-Cutting*," *U.S. Naval Institute Proceedings*, January 1900, *26* (1), 157–166. Vol. 26/1/93.

__ , "*Cable Cutting*," *U.S. Naval Institute Proceedings*, January 1904, *30* (1).

Headrick, Daniel R., *The Tools of Empire: Technology and European Imperialism in the Nineteenth Century*, New York: Oxford University Press, 1981.

__ , *The Invisible Weapon: Telecommunications and International Politics, 1851-1945*, OUP USA, 1991. Google-Books-ID: UDXnCwAAQBAJ.

Hinsley, F. H., *British Intelligence in the Second World War: Its Influence on Strategy and Operations*, New York: Cambridge University Press, 1979.

Hjort, Jonas and Lin Tian, "The Economic Impact of Internet Connectivity in Developing Countries," *Annual Review of Economics*, August 2025, *17* (1), 99–124.

Hochfelder, David, *The Telegraph in America, 1832–1920*, Baltimore: Johns Hopkins University Press, 2013.

Imbs, Jean and Laurent Pauwels, "Mapping the Global Submarine Cable Network: Resilience, Vulnerability, and Geopolitics," 2026. Working paper, NYUAD.

International Cable Protection Committee, "Cableships of the World," `https://www.iscpc.org/information/cableships-of-the-world/` 2025. Accessed March 2026.

Juhász, Réka and Claudia Steinwender, "Spinning the Web: The Impact of ICT on Trade in Intermediates and Technology Diffusion," Technical Report w24590, National Bureau of Economic Research, Cambridge, MA May 2018.

Kennedy, P. M., "Imperial Cable Communications and Strategy, 1870–1914 1," in "The War Plans of the Great Powers (RLE The First World War)," Routledge, 2014. Num Pages: 24.

Kimball, William W., "*Plan of Operations Against Spain*," 1896.

Kunert, A., *Telegraphen-Seekabel*, Vol. 2 of *Geschichte der deutschen Fernmeldekabel*, Deutsch-Atlantische Telegraphengesellschaft, Koeln, and Norddeutsche Seekabelwerke A.-G., Nordenham, 1962.

Mohr, Cathrin and Christoph Trebesch, "Geoeconomics," *Annual Review of Economics*, 2025, *17* (1), 563–587.

Murphy, Erin L. and Matt Pearl, "China's Underwater Power Play: The PRC's New Subsea Cable-Cutting Ship Spooks International Security Experts," April 2025.

Naval Association of Australia, "*Monthly Ceremony: Jack's Memorial Southbank*," Event handout /

commemorative pamphlet November 2020.

Ocon, Jaime and Jonathan Walberg, "*China's Undersea Cable Sabotage and Taiwan's Digital Vulnerabilities*," *Global Taiwan Brief*, 2025, *10* (11). Published by the Global Taiwan Institute; accessed 2026-03-19.

O'Connell, John F., "*German Special Submarine Operations During WW I*," *The Submarine Review*, April 2010.

Peters, Benjamin, *How Not to Network a Nation: The Uneasy History of the Soviet Internet*, The MIT Press, March 2016.

Royal Navy, "*Admiralty's War Diary World War Two*," n.d. Collection page for the Second World War Admiralty War Diaries.

Sontag, Sherry and Christopher Drew, *Blind Man's Bluff: The Untold Story of American Submarine Espionage*, New York: HarperTorch, 1999.

Starosielski, Nicole, *The Undersea Network*, Duke University Press, 2015.

Steinwender, Claudia, "Real Effects of Information Frictions: When the States and the Kingdom Became United," *American Economic Review*, March 2018, *108* (3), 657–696.

Subramanian, Samanth, *The Web Beneath the Waves: The Fragile Cables that Connect Our World*, Columbia Global Reports, 2025.

Sutherland, Ewan, "*The Yi Peng 3 and Eagle S incidents - cutting cables in the Baltic Sea*," in "33rd European Regional ITS Conference, Edinburgh, 2025: Digital innovation and transformation in uncertain times" International Telecommunications Society (ITS) Edinburgh 2025. Conference paper.

United States. Navy Department. Bureau of Navigation, *Appendix to the Report of the Chief of the Bureau of Navigation: Naval Operations of the War with Spain*, Washington, D.C.: United States Government Printing Office, 1898. Digitized by The Portal to Texas History.

Wheeler, Tom, *Mr. Lincoln's T-Mails: The Untold Story of How Abraham Lincoln Used the Telegraph to Win the Civil War*, New York, N.Y: Harper Business, 2006.

Wilson, Herbert Wrigley, *The Downfall of Spain: Naval History of the Spanish-American War*, London: Sampson Low, Marston & Company, Limited, 1900.

Winkler, Jonathan Reed, *Nexus: Strategic Communications and American Security in World War I*, Harvard University Press, 2008.

8 Appendix

8.1 Empirical Implementation of the Traffic Assignment model

As discussed in Section 4, the exogenous ingredients of our traffic assignment model and the variables we create are the OD matrix $(Flow)_{o\in I,d\in I}$, the transportation-cost vector $(Distance)_{\ell\in L}$, and the number of cables per corridor $NumCables_\ell$. The objective of this section is to describe how we measure each of these objects.

8.1.1 Data flows ($Flow_{od}$)

Because data on country-to-country data flows is scarce, especially across 150 years, we proxy the OD matrix of bilateral data flows with bilateral trade flows. For this purpose, we use long-run bilateral trade data from the widely used TradeHist dataset, complemented with data from the RICardo datasets to fill coverage gaps in the 19th century and IMF and World Bank data from 2015 until 2020 (more specifically, we build on the compilation in Broner, Martin, Meyer and Trebesch 2025. See that paper for further details).

One reason to expect trade to be a good proxy for data flows is that there is a causal link from trade to data: commercial exchange generates digital communication, whether through supply chain coordination, logistics, remote management, or financial transactions. Countries that trade more are likely to communicate more, which would create higher bilateral data flows. Second, even in the absence of a direct causal mechanism, trade and data flows are shaped by similar structural forces such as population, GDP, geographic distance, language and cultural affinity, and historical ties.

The main drawback of relying on trade flows is that they weight transactions based on their value. Clearly, the same amount of value of trade in manufacturing may induce different data flows than the same value of trade in services. Nevertheless, in light of current data limitations, we maintain that trade flows are the best available proxy for data flows. Unfortunately, however, direct measures of data flows are noisy, are only available for the last decade, and are mostly focused on tracking large data flows.

Our assumption of approximating data flows with trade flows delivers a global, historical panel of bilateral flows, spanning the full period for which we observe telecommunication infrastructure. Additionally, we assume that every data flow originates from or is destined to the capital city of each country.

8.1.2 Transportation Cost ($Distance_\ell$) and Number of Cables ($NumCables_\ell$)

Rather than using the actual submarine network, we derive the transportation cost vector from a simplified network (the corridors network). Such network consists of 24 distinct nodes, which we call data hubs (e.g., New York, San Francisco, Lisboa, Tokyo), 35 corridors connecting the data hubs, of which 26 are submarine (e.g., New York-Lisboa or San Francisco-Tokyo) and 9 terrestrial (e.g., New York-San Francisco). As each corridor ℓ is identified by the data hubs it connects, we let $Distance_\ell$ be the geodesic distance in kilometers between them. Table 8 lists all corridors between data hubs, whether they are terrestrial or submarine, and their distance attribute. In addition to these corridors, we assume that every capital city (the origin and destination of the data flows) is connected via a generic reserved terrestrial link to the closest data hub (whenever possible), and we assume that any two capital cities that are assigned to the same data hub are connected via a generic reserved terrestrial link (whenever possible). Finally, we calculate $NumCables_\ell$ as the sum of all active cables assigned to corridor ℓ, where we assign cables to corridors by attributing each landing point to the closest data hub and thus identifying the corridor (pair of data hubs) served by that cable.

To understand why we aggregate at the level of the corridors, rather than directly using our data on cables, note that the cables network is very dense, with multiple landing points in each country. At the same time, we do not know the exact origin and destination of the data flows and we do not observe the country's domestic and terrestrial networks. To see why this can be problematic, suppose that France and the United States are connected by a cable that connects Brest and New York and another cable that connects Nantes and Atlantic City. If we applied a shortest-path algorithm to determining which of the two cables is used, the answer would heavily depend on our assumption that the data flows between the US and France travel between Paris and Washington DC and it would then also be very sensitive to what we assume about how New York and Atlantic City are connected to Washington DC or how Brest and Nantes are connected to Paris. On the other hand, our approach is more robust as it would assign both these cables to the Amsterdam-New York corridor and they would thus be assumed to face the same amount of traffic regardless of our exact assumptions on origin-destination cities and domestic networks.

Table 8

Node1	Node2	Type	Corridor description	Region	Distance (km)
Alexandria, EGY	Suez, EGY	Terrestrial	links Europe Mediterranean & Asia South West		160
Amsterdam, NLD	Marseilles, FRA	Terrestrial	links Europe Mediterranean & North		900
Brisbane, AUS	Tahiti, PYF	Submarine	Oceania	Asia	7050
Cape Town, ZAF	Durban, ZAF	Terrestrial	links Africa South-East & South-West		1260
Cape Town, ZAF	Lagos, NGA	Submarine	Africa West	Africa	4560
Caracas, VEN	Recife, BRA	Submarine	America South-Atlantic	America	4440
Durban, ZAF	Mombasa, KEN	Submarine	Africa East	Africa	3040
Durban, ZAF	Singapore, SGP	Submarine	links Africa East & Asia South-East	Trans-Indian	7280*
Hong Kong, CHN	San Francisco, USA	Submarine	links Americas & Asia South-East	Trans-Pacific	11140*
Hong Kong, CHN	Tianjin, CHN	Submarine	links Asia East & Asia South-East	Asia	1890
Lagos, NGA	Lisboa, PRT	Submarine	links Africa West & Europe	Africa	4310
Lisboa, PRT	Amsterdam, NLD	Submarine	links Europe Atlantic & North	Europe	2190
Manta, ECU	Maracaibo, VEN	Terrestrial	links America Caribbean & South-Pacific	Africa	1830
Manta, ECU	San Francisco, USA	Submarine	links America North-West & America South-West	America	5120
Maracaibo, VEN	Caracas, VEN	Terrestrial	links America Caribbean & South-Atlantic		520
Marseilles, FRA	Alexandria, EGY	Submarine	Europe Mediterranean	Europe	2080
Marseilles, FRA	Lisboa, PRT	Terrestrial	links Europe Atlantic & Mediterranean		1470
Miami, USA	Maracaibo, VEN	Submarine	America Caribbean	America	1840
Mombasa, KEN	Suez, EGY	Submarine	links Africa East & Asia South-West	Africa	3500
Mumbai, IND	Singapore, SGP	Submarine	links Asia South-East & Asia South-West	Trans-Indian	3910
New York, USA	Lisboa, PRT	Submarine	links America North & Europe Atlantic	Trans-Atlantic	5450
New York, USA	Miami, USA	Terrestrial	links America North-East & Caribbean		1760
New York, USA	Recife, BRA	Submarine	links America North-East & South-Atlantic	America	6740
New York, USA	San Francisco, USA	Terrestrial	links America North-East & North-West		4130
Recife, BRA	Lagos, NGA	Submarine	links Americas & Africa West	Trans-Atlantic	5250
Recife, BRA	Lisboa, PRT	Submarine	links America South-Atlantic & Europe	Trans-Atlantic	5660
San Francisco, USA	Miami, USA	Terrestrial	links America North-West & Caribbean		4160
Santiago, CHL	Manta, ECU	Submarine	America South-Pacific	America	3640
Singapore, SGP	Brisbane, AUS	Submarine	links Asia South-East & Oceania	Asia	6150
Singapore, SGP	Hong Kong, CHN	Submarine	Asia South-East	Asia	2580
Suez, EGY	Mumbai, IND	Submarine	Asia South West	Trans-Indian	4410
Tahiti, PYF	Santiago, CHL	Submarine	links Americas & Oceania	Trans-Pacific	8420*
Tianjin, CHN	Tokyo, JPN	Submarine	Asia East	Asia	2100
Tokyo, JPN	Brisbane, AUS	Submarine	links Asia East & Oceania	Asia	7100*
Tokyo, JPN	San Francisco, USA	Submarine	links America North & Asia East	Trans-Pacific	8270*

Note: distances marked with an asterisk (*) are assumed to be infinite prior to 1902, the year of the first successful installation of a Trans-Pacific cable. Terrestrial links are not assigned a Macro-region as we do not observe terrestrial cables. For compactness, we pool together Asia and Oceania in our definition of regions. We omit the Trans-Siberian terrestrial corridor as it consists of cables with relatively low capacity (https://www.submarinenetworks.com/).