Daniel Andrés Birchner 18/1/2025

INTRODUCTION TO A GEOPOLITICS OF CYBERSPACE

Talking about cyberspace initially means referring to a virtual, intangible space where global information interconnections, computer systems, and databases converge. William Gibson popularized the term in his 1984 cyberpunk novel Neuromancer, where he described cyberspace as a kind of "*consensual hallucination*"—a non-physical space in which millions of people interact through computer networks. This early conception gave rise to the germinal idea of a shared digital environment that transcends geographical distance in real time and on a massive scale. In 2001, the Royal Spanish Academy included the term in its 22nd edition, defining it as a "*virtual environment created by computer means*."

Several scholars in the field have added layers to these definitions as they examined different dimensions of cyberspace, including the dynamics of the relationships it enables. Manuel Castells, in *The Rise of the Network Society* (1996), emphasized cyberspace as the spatial logic of the network society, highlighting its role in reshaping social control and exchanges. From a more cultural standpoint, Pierre Levy in *Cyberculture* (1997) argued that "*Cyberspace is an interactive communication medium that is not limited to a physical substrate… …and it expands humanity's cognitive, imaginative, and communicative capacities.*" In this way, Levy stressed its transformative potential in enabling relational and cultural dynamics specific to the digital realm, going beyond geographic, legal, and physical limitations.

The concept, originally born in science fiction, has become progressively normalized in popular language as more aspects of daily life—such as communication, commerce, and resource management—have been digitized. The definitions presented so far agree that cyberspace is:

- A permanent space for the circulation and exchange of digital data
- Virtual and intangible

- Supra-geographical and supra-legal
- A social, cultural, and political environment
- A space where new relationships emerge between individuals, corporations, and governments
- An environment in which control is exercised differently than in the physical world

To these perspectives, we can add NATO's definition, which emphasizes the role of cybersecurity and defense policies:
"Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

This final definition underscores cyberspace's reliance on physical infrastructure—without which it could not exist as we know it. This relationship between the virtual and the tangible lays the foundation for a **Geopolitics of Cyberspace**, with two main dimensions: a geographic one (related to the location of infrastructure) and a political one (related to its regulation and control).

From a **geographic standpoint**, this physical infrastructure is distributed globally according to various criteria—such as climate conditions (e.g., temperature and humidity requirements for servers and data centers) and accessibility (submarine cables connect to land via coastal landing stations). Antennas, submarine cables, servers and data centers (some of them underwater), coastal landing stations, and other components all have owners—whether state or private—and are subject to the sovereignty of the countries in which they are located. This means that control over infrastructure also extends to certain dimensions of cyberspace. And this is an increasing trend: more and more domestic technologies are connected to the Internet of Things, while many countries are digitizing large portions of their bureaucracy and critical infrastructure management. Not to mention the fact that the development and growing use of artificial intelligence will require an even larger and more complex physical cyberspace infrastructure.

In this context, one striking fact is that much of this infrastructure is privately owned. A key example is submarine cables, through which 95% of current internet and telephone data flows[1]. The transition from copper submarine cables to fiber optics began in 1988 with the TAT-8 cable (linking the United States with France and the United Kingdom), built by a consortium of telecommunications companies led by AT&T. This new technology responded to the rising volume and quality of data transmission and coincided with the spread of domestic phone lines (later, it became the first cable to transmit private internet data, mainly email). Since then, only around 20% of the world's submarine cables are state-owned, with 59% in private hands and the remainder controlled by small consortia and other entities. Submarine cables now offer the best performance in terms of capacity and quality. The growing need for connectivity, as well as increasing demand for data volume and processing speed (facilitated by artificial intelligence), means greater bandwidth and lower latency, outcompeting other data traffic systems such as satellites. We are moving toward a world of more and better submarine cables—and this increasing dependence may also turn them into attractive military targets.

Another interesting case is that of coastal landing stations—facilities on land that receive submarine cables and adapt the data flow for continental fiber optic networks. Countries that possess these stations enjoy a strategic advantage over landlocked nations that must rely on neighbors or satellite links for internet access. For example, countries like Afghanistan, Armenia, Moldova, Nepal, Bhutan, and Kosovo depend either on their neighbors or on satellites. Others are vulnerable due to having only a single connection (in this case, terrestrial fiber optics), such as Yemen and Somalia. A direct attack on that single communication channel would digitally isolate those countries. Notably, some of the aforementioned nations do have coastlines but lack landing stations. Other landlocked countries—such as the Czech Republic and Switzerland—are connected by multiple terrestrial cables to different nations, ensuring connection redundancy in the event of armed conflict, failure, or sabotage[2].

---

[1] World Map of Submarine Cables – https://www.submarinecablemap.com/

[2] *Submarine Cables: The True Communication Highway*, Mapfre Global Risks – https://www.mapfreglobalrisks.com/en/risks-insurance-management/article/submarine-cables-the-true-communication-highway/

From a **political standpoint**, the Geopolitics of Cyberspace addresses the study of the laws and regulations that states or international organizations apply to cyberspace. Data governance, cyber diplomacy, cybersecurity, cyber intelligence, and digital sovereignty are all expressions of the control and regulation exercised by states, multinational corporations, and international bodies over the production, circulation, storage, and use of digital information.

The fundamental power of national states and international organizations, in relation to the geopolitics of cyberspace, lies in their legislative capacity. Regarding data governance, several governments and international entities have established regulatory frameworks—such as the European Union's GDPR (General Data Protection Regulation), which aims to protect users' privacy online by regulating how private companies and social media platforms use and transfer data. Another example is the CLOUD Act (2018)[3] in the United States, which allows U.S. authorities to access data stored on servers owned by tech companies, even if those servers are located outside of U.S. territory. This is a clear example of the transnational nature of data and legal reach.

As for Digital or Cyber Sovereignty, this refers to a state's right to exercise control and authority over the activities, infrastructure, and data within its digital territory. The People's Republic of China exercises cyber sovereignty through its Great Firewall, which filters and regulates internet access within its borders. Another example is Russia's Runet, a project still in testing stages that seeks to control internal internet connectivity and reduce dependence on foreign providers. In 2024, successful tests were conducted in the Caucasus region (Dagestan, Ingushetia, and Chechnya), temporarily disconnecting this zone from the global internet. During this test, messaging services and certain websites became inaccessible to the local population.

Finally, in the political dimension, Cyber Diplomacy refers to the framework of international cooperation in which states design, coordinate, and implement strategies to manage their interests in cyberspace. Among these strategies are joint approaches to

[3] CLOUD Act: Clarifying Lawful Overseas Use of Data.

cybersecurity and cyber intelligence, data governance, legislation on tech monopolies, and international response mechanisms to threats and transnational actors.

Cyberspace, then, is a dimension that can be affected not only in digital or intangible ways, but also through control over its physical infrastructure. Sabotage of submarine cables, hacking (or destruction) of communication satellites, destruction of antennas, data storage laws, anti-monopoly regulations, restrictions on access to certain websites, or the provision of a national intranet independent from external services are all examples of how, both physically and legally, cyberspace becomes a territory in which states, organizations, and users pursue their interests.

With that in mind, today we find numerous examples that highlight not only the relevance but also the growing trend of cyberspace as a pressure arena. Below, we focus on incidents in which the manipulated component was primarily physical—not because it is more important, but because, among the literature consulted for this article, it remains the least explored aspect from a geopolitical perspective.

In November 2024, the Chinese ship Yi-Peng 3 was involved in an international scandal when its route through the Baltic Sea coincided with the location of two damaged submarine fiber optic cables[4]. Both cables were damaged within 24 hours—a time frame in which the Chinese vessel was present in the area. The Chinese government promptly cooperated with the investigation led by Swedish authorities, who did not issue a formal accusation as the case remained open. The result was a temporary outage in telephone service in Sweden and Lithuania, with the latter losing a third of its internet capacity. Both cables were restored by the end of that month. Since the Chinese vessel had previously docked in Saint Petersburg, Russia, speculation arose around the possibility of a "sabotage rehearsal."

And this is not the only case involving Russia. Within the current context of the war in Ukraine and growing concern about Moscow's posture toward Europe, in June 2023, former president and current deputy chairman of Russia's Security Council, Dmitry Medvedev, stated that there was no reason Moscow should refrain from destroying

[4] The damaged cables were C-Lion 1 (Germany–Finland) and BCS East-West Interlink (Lithuania–Gotland Island, Sweden).

enemy submarine cables[5]. This statement was framed as a response to the alleged involvement of Western countries in the September 2022 sabotage of the Nord Stream underwater gas pipeline[6]. Although the latter concerns gas infrastructure, it exposed the vulnerability of submarine installations—fiber optic cables included. Moreover, in May 2023, NATO reported the presence of Russian ships and submarines in areas with high concentrations of cables in Northern Europe and North America, raising suspicions of Moscow's mapping activities of communication infrastructure[7].

In this context, Russia's geography offers a clear advantage. Due to its continental position, Russia relies predominantly on terrestrial infrastructure for its information systems. Countries such as the United Kingdom, Taiwan, the Baltic States, Japan, and South Korea (along with other continental allies) are particularly vulnerable to attacks on their submarine cables, even though they possess redundant systems. That said, in a probable future where the physical infrastructure of cyberspace becomes a regular military target, Russia would be less exposed—something that even the United States and its Western allies could not claim. Similar concerns arose in April 2024, when, according to the website Aviation24.com[8], commercial airplanes flying over the Baltic Sea experienced anomalous fluctuations in their GPS navigation systems—some of which had to make emergency landings. Official sources in Lithuania linked these incidents to Russian jamming[9] capabilities in neighboring Kaliningrad, where Moscow maintains fixed electronic warfare facilities.

These cases demonstrate that threats to cyberspace infrastructure demand cooperation between private companies, which own much of the infrastructure, and national governments, which are the only actors capable of providing military protection—

---

[5] *Medvedev: Moscow Now Has Free Hand to Destroy Enemies' Undersea Infrastructure,* Reuters, June 2023 – https://www.reuters.com/world/europe/russias-medvedev-says-moscow-now-has-free-hand-destroy-enemies-undersea-2023-06-14/

[6] The Nord Stream system includes four pipelines divided between two routes, Nord Stream 1 and Nord Stream 2. At the time of the explosions, none were operational, but still contained residual gas that escaped to the sea surface.

[7] In October 2023, another cable linking Estonia and Sweden was damaged, in a region previously navigated by Russian vessels.

[8] *Widespread GPS Interference Grips European Airspace; Suspicions Rise Over Russian Involvement*, Aviation24.com – https://www.aviation24.be/airlines/widespread-gps-interference-grips-european-airspace-suspicions-rise-over-russian-involvement/

[9] Jamming: A term referring to interference, denial, or saturation of transmission systems such as radar, radio, or GPS.

something private companies cannot do[10]. In this regard, political factors also come into play, through the regulations and controls that states impose on such infrastructure to safeguard it from foreign actors or harmful interference. However, we must remember that many of these cables cross international waters, which are legally beyond state jurisdiction and extremely difficult to monitor.

In the West, the Chinese company Huawei has been at the center of geopolitical debate, due to suspicions that its provision of 5G services in European countries and the United States (which involves the installation and maintenance of antennas) could have hidden espionage purposes. In this context, the U.S. government claimed the company posed a threat to national security and banned Huawei equipment in 2019. The United Kingdom also prohibited the company's participation in its 5G network, demanding the complete removal of its equipment by 2027. Australia adopted similar measures, and Canada followed suit in 2022. The cooperation between these countries—based on intelligence sharing—means that a vulnerability in one could represent a threat to the rest. In addition, Washington imposed sanctions on semiconductor suppliers, banning the sale of advanced chips to Huawei. Indirectly, the production and distribution of semiconductors, given their relevance to the physical infrastructure of cyberspace, also emerges as a critical issue in the Geopolitics of Cyberspace[11].

As there are threats, there are also efforts to counter them. Returning to the case of submarine cables, digital monitoring systems are being tested in Northern Europe to quickly detect anomalies on the seafloor—potential signs of human intervention targeting underwater infrastructure. This is complemented by temporary redundancy measures[12], such as backup cables or private satellite networks, like Elon Musk's

[10] *Safeguarding Subsea Cables: Protecting Cyber Infrastructure Amid Great Power Competition,* CSIS – https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

[11] *US-China Tech Rivalry and Submarine Cables*, Reuters Investigates – https://www.reuters.com/investigates/special-report/us-china-tech-cables/

[12] Satellites cannot handle nearly the same volume of data as submarine cables. Therefore, they are considered temporary redundancy measures, prioritizing strategic or national security communications in case of cable destruction or denial.

Starlink, Amazon's Kuiper, or the UK's OneWeb[13].

Cyberspace reveals itself as a domain where military, psychological, and intelligence strategies can be executed just as they are in the physical world. While it is an intangible space, it cannot exist without its physical infrastructure, which is itself shaped by geography and regulation. And since most of this infrastructure is privately owned, cooperation between telecommunications companies and governments able to provide protection is vital. Yet, as previously noted, much of this infrastructure lies outside the legal reach of states, in international zones that are hard to trace and even harder to repair.

Our dependence on these systems will only grow. And the physical—and to a lesser extent, political—infrastructure of cyberspace will take on an increasingly central role in 21st-century geopolitical disputes.

[13] *Elon Musk's Starlink Won't Replace Undersea Cables,* Business Insider – https://www.businessinsider.com/elon-musk-starlink-satellite-internet-undersea-cables-not-extinct-tonga-2022-2