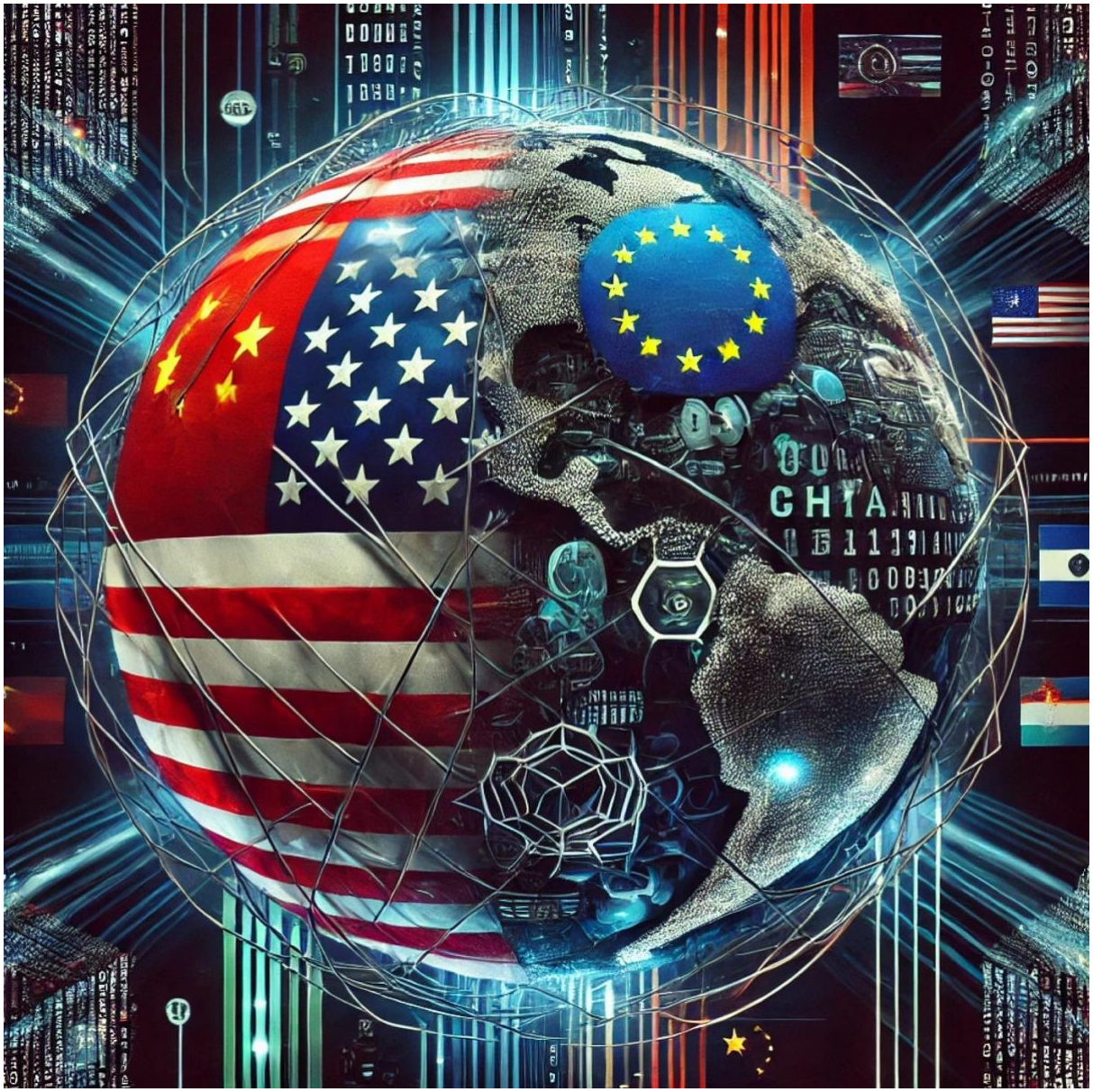

Forum:	The Fourth General Assembly
Issue:	Ensuring Digital Sovereignty and Addressing Neo-Colonialism in Cyberspace
Student Officer:	Santiago Fattoruso
Position:	Deputy President

Introduction

The last century was defined by countries fighting for their independence, breaking away from empires to control their own land and borders. However, the twenty-first century has brought a new and quieter struggle: the fight for control over the digital world. Today, being connected to the internet is essential for any country to survive economically. Yet the way this connection is built is creating a situation that looks a lot like the colonialism of the past. This is often called "digital neo-colonialism," and it threatens to make the independence of developing nations meaningless if their internet systems and citizens' data are owned and controlled by foreign powers.

The main problem this report will explore is the difficult choice facing many developing nations. To grow their economies, they need fast internet, 5G networks, and modern technology right now. But because they often cannot build these systems themselves, they have to rely on powerful technology from countries like China or the United States. This dependence gives outside powers huge influence over national security and economic growth. It effectively turns data into a new natural resource that is taken from the developing world to benefit others. This research report will examine how this dependency works, look at the competition between major tech powers, and discuss how the international community can ensure every nation has true control over its own digital future.

Key Terms

Digital sovereignty

The right of a state to govern the internet within its borders, including control over digital infrastructure, citizen data, and applicable laws, similar to physical border control.

Fiber-optics

Thin glass fibers that transmit light signals, serving as the main foundation of the internet to carry vast amounts of data at high speeds across oceans.

Data localization

Regulations requiring that data about a nation's citizens be collected, processed, and stored on servers physically located inside that country to ensure local legal jurisdiction.

The “Digital Silk Road”

A Chinese state-led initiative to build internet infrastructure like underwater cables and 5G networks in developing nations.

Neo-colonialism

Using economic or technological pressure rather than military force to influence other countries. In this context, it refers to powerful nations controlling the digital systems of developing states.

5G networks

The fifth generation of mobile technology designed to connect people and machines.

Data centers

Large physical facilities used to house critical computer systems and data. They are the "brains" of the internet.

General Overview

To really understand the issue of digital neo-colonialism we first have to look past the screen and understand how the internet actually works. We often think of the internet as a "cloud" or something invisible that is everywhere at once. But in reality, the internet is physical. It is made up of thousands of miles of fiber-optic cables running under the oceans and heavy servers stored in massive warehouses. The way this physical infrastructure was built is the root of the problem today. Historically, when colonial powers built railways in Africa or Asia, they didn't build them to connect local cities to one another. They built them to connect mines and large farms directly to the ports so resources could be shipped back to Europe.

this colour

Origin

The map of the global internet looks very similar to those old colonial maps. For a long time, internet traffic from one African country to its neighbor had to travel all the way to London or Paris and back simply because the cables were not laid to connect the region internally. This lack of infrastructure left a massive gap in the system. Developing nations needed to modernize quickly to catch up with the global economy but they lacked the money and the technology to lay these cables themselves. This opened the door for foreign powers to step in. They arrived not just as helpers but as owners of the basic systems that run these countries. This is where the modern issue begins as we see a transition from extracting physical resources to extracting digital ones.

Data mining

The core of the debate today is about how data has become the world's most valuable resource. In the digital economy every time a person uses a smartphone or buys something online, they are generating data. In the current global system this "raw material" is extracted from developing nations on a massive scale. Citizens in the Global South use apps and platforms owned by American or Chinese companies and their data is instantly transferred out of their country. It is processed in data centers in the United States or China where it is used to train Artificial Intelligence and improve algorithms.

The problem is that the economic value of this data stays in the North. The developing nation provides the raw material but has to buy back the finished product at a premium. This creates a permanent trade deficit. Just as colonies once exported cotton and imported expensive clothes digital colonies export data and import expensive software services. This cycle prevents local tech companies from growing because they cannot compete with the massive giants from overseas who already own the infrastructure and the user base.

Global competition

This situation is complicated by the intense rivalry between the United States and China which puts developing nations in a very difficult position. This is often called the "Great Tech War." On one side there is the "Digital Silk Road" promoted by China. Chinese companies like Huawei and ZTE offer developing nations a deal that looks very good. They will build 5G networks and data centers cheaper and faster than anyone else often backed by the Chinese

government. For a country like Ethiopia or Pakistan this is a lifeline that allows them to modernize their economy. However Western nations argue that this creates a "debt trap" and gives the Chinese government potential access to spy on sensitive communications.

On the other side the Western model is driven by private corporate giants like Google and Amazon. While these are not owned by the state their influence is just as powerful. These companies often have more money than the countries they operate in. They dominate the "platform layer" of the internet. For example, in some countries Facebook effectively is the internet for the average user. The concern here is "corporate colonialism." These companies often lobby against laws that would force them to store data locally because they believe the internet should be borderless. However, if a country's public discussions happen on American servers and its government data is stored in a foreign cloud that country loses the ability to enforce its own laws.

The current struggle for sovereignty

Right now, we are seeing a major shift as developing nations try to fight back. This has led to the rise of "digital sovereignty" as a key political goal. Countries are realizing that if they don't own their technology, they don't own their future. We are seeing nations in the "Digital Non-Aligned Movement" trying to create a third way. They are attempting to pass "data localization" laws which are rules requiring that citizens' data must be stored on servers physically located inside the country.

However, the reality on the ground is challenging. Building a local internet ecosystem requires three things that are scarce in the Global South: massive amounts of capital, reliable electricity grids to run data centers, and highly specialized engineers. Because of this even when countries want to break free, they often find themselves forced back into dependency. They might pass a law to keep data local but then realize they have to hire a foreign company to build the data center to store it. The debate effectively stands at a crossroads. Can developing nations build their own digital walls to protect their economy or will the internet continue to be divided into areas of control managed by the world's superpowers?

Major Parties Involved

The People's Republic of China

China is currently the most active builder of internet systems in the developing world. Through its "Digital Silk Road" project the Chinese government supports major companies like Huawei and ZTE to enter markets in Africa, Asia, and Latin America. Their approach focuses on "hard infrastructure." They build the cell towers, lay the underwater cables, and supply the surveillance cameras that developing nations need. Because these projects are often funded by the Chinese government, China can offer prices that Western companies usually cannot match.

For the Chinese government this is not just about business. It is about setting the standards for how the internet works in the future. By building the networks that other countries run on Beijing ensures that its technology becomes the default choice. This creates a long-term relationship where the receiving country relies on Chinese updates and technicians to keep their internet running. China argues that they are simply helping nations that the West ignored for decades. However, critics in the UN often debate whether this assistance comes with political expectations. Western nations frequently raise concerns that this equipment could be used for espionage although China strongly denies this.

The United States of America

The United States represents the other major power in this debate, but its influence comes from a different source. While China builds the physical cables American companies own the platforms that people actually use. Giants like Google, Amazon, Microsoft, and Meta (Facebook) are all based in the US. This gives the United States immense influence over global culture and economy. The US government generally argues for the "free flow of data." They believe that the internet should not be broken up by national borders. This policy benefits American companies because it allows them to operate freely in every country without having to build expensive local servers in each one.

However, the US government also uses control through laws like the CLOUD Act. This law allows American law enforcement to request data held by US companies even if that data is stored on a server in a foreign country. This has caused tension with other nations who feel that American laws should not apply to their citizens. For the United States the priority is maintaining an open global internet where its technology sector can continue to lead while simultaneously trying to limit the use of Chinese hardware in allied nations.

The Republic of India

India has emerged as the leading voice for the Global South in the debate over digital sovereignty. As a country with a huge population but a developing digital economy India has taken a strong position against both American "data colonization" and Chinese security threats. The Indian government has argued that data is a national asset. They famously described data as the "new oil" that should benefit Indian citizens rather than foreign corporations. To enforce this India has proposed strict laws that would force foreign tech giants to store payments and personal data within India.

India is also unique because it has taken direct action against the big tech powers. It banned hundreds of Chinese apps including TikTok citing national security concerns and has frequently clashed with American companies like Twitter over government regulation. For many developing nations in Africa and Southeast Asia India serves as a model for how to push back against the superpowers. They look to India to see if it is possible to build a "self-reliant" digital economy without completely cutting ties with the global market.

Timeline of Key Events

September 2013	Chinese President Xi Jinping launches the Belt and Road Initiative. This massive project eventually includes the "Digital Silk Road," marking China's first move towards creating internet infrastructure across the Global South.
December 18th 2013	The United Nations General Assembly adopts its first resolution (Resolution 68/167) specifically focused on the right to privacy in the digital age. This was a direct response to global concerns about mass surveillance and international interference in national data.
May 2015	China officially adds the "Information Silk Road" to its global strategy.
March 23rd 2018	The United States passes the CLOUD act, allowing its government to access data stored by American companies regardless of in which part of the world it is located.
April 6th 2018	India issues a strict directive (Reserve Bank of India Data Directive), requiring all payment system providers to store their transaction data only within India. This is one of the first major examples of a developing nation using law to keep its citizens' data out of other nations' hands.
August 11th 2023	India issues the Digital Personal Data Protection Act that establishes clear rules for how the data of its 1.4 billion citizens is handled. It creates a framework for "digital sovereignty" that many

other developing nations are now looking to copy.

Previous Attempts to solve the Issue

UN General Assembly Resolution 68/167 (The Right to Privacy in the Digital Age)

This resolution was an important moment for the United Nations because it formally established that the human rights people have offline also should be implicated in online situations. This idea and resolution started with people being frustrated regarding mass surveillance by foreign intelligence agencies. While this resolution is not a binding law that forces countries to change their behavior, it had a very impacting diplomatic effect. It gave developing nations an official resolution they could refer to, in order to challenge the oppression of digital superpowers. Before this, there was little agreement on digital rights, but this document clarified that privacy is a universal right, serving as a foundation for future data protection laws.

The OECD Guidelines on the Protection of Privacy and Transborder Flows

The Organization for Economic Co-operation and Development (OECD) created these guidelines to solve the difficult problem of how data moves between countries. In a global economy, businesses need to move information across borders, but nations also need to protect their citizens' privacy. The main idea of the OECD Guidelines is to find a balance between the "free flow of information" and personal security. They set the standard for many Western nations by making nations responsible: even if data leaves a country, the organization moving it is still responsible for its safety. This framework remains a key reference point for international data agreements.

The African Union Convention on Cyber Security and Personal Data Protection

Also known as the "Malabo Convention," this treaty is a vital attempt by the African Union to defend their continent digitally. Its purpose is to create a set of rules that are implied in every country, so

that every African nation has the same rules and perspective for data protection. The intention is to stop foreign tech companies from taking advantage of nations with lax laws while avoiding those with strict ones. African states hope to gain power by cooperating and adopting common regulations, which will enable them to deal with multinational tech companies as a group rather than as vulnerable individual countries.

Possible Solutions

The third way through an infrastructure fund

One of the main reasons developing nations turn to China's "Digital Silk Road" is that they lack the money to build their own networks. Western lenders often view these infrastructure projects as too risky. A strong solution would be for the United Nations, in partnership with the World Bank, to create a global "Digital Infrastructure Fund." This fund would remain open and neutral while offering low-interest loans specifically for the construction of fiber-optic cables and 5G networks. This would give developing nations a third option, as they wouldn't have to choose between expensive American corporations or Chinese state-surveillance. It would allow them to build the hardware they need without selling their digital sovereignty to a superpower.

Capacity building and technology transfer

A major cause of digital dependence is the lack of human experience. Many developing nations rely on foreign tech superpowers, simply because they do not have enough local engineers to run their own systems. A constructive solution is to focus on UN funded/supported education and training programs. The goal would be to educate people all around the world on how these systems work. By training local data technicians, the UN can help developing nations build a workforce capable of managing their own internet.

Harmonized global data standards

Currently, the world has many different data laws, which can lead to confusion and possible exploitation. A general solution is for the UN to create common and agreed upon standards for data protection. This strategy emphasizes openness and diplomacy rather than harsh prohibitions or high taxes. The goal is to create a set of universally accepted guidelines for the processing and tracking of data that crosses international borders. This allows global internet to remain accessible, while giving smaller nations the assurance that their citizens' data is being treated with a minimum standard of respect, regardless of where it is processed.

Bibliography

"Building Tomorrow's Digital Public Infrastructure." *Chatham House – International Affairs Think Tank*, 13 Jan. 2026, www.chathamhouse.org/events/all/standard-event/building-tomorrows-digital-public-infrastructure. Accessed 19 Jan. 2026.

"China's Digital Silk Road." *Www.csis.org*, Feb. 2019, www.csis.org/analysis/chinas-digital-silk-road.

"China's Digital Silk Road: Integration into National IT Infrastructure and Wider Implications for Western Defence Industries." *IISS*, www.iiss.org/research-paper/2021/02/china-digital-silk-road-implications-for-defence-industry/.

"Data Colonialism and Data Sets." *Harvard Law Review*, 22 June 2023, harvardlawreview.org/blog/2023/06/data-colonialism-and-data-sets/.

"Digital Sovereignty and Data Colonialism: Shaping a Just Digital Order for the Global South." *Policy Center*, 2025, www.policycenter.ma/publications/digital-sovereignty-and-data-colonialism-shaping-just-digital-order-global-south.

"Foresight Africa 2024." *Brookings*, www.brookings.edu/collection/foresight-africa-2024/.

"Global Risks Report 2023 | World Economic Forum." *World Economic Forum*, 2023, www.weforum.org/publications/global-risks-report-2023/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities/.

Hicks, Jacqueline. "'Digital Colonialism': Why Some Countries Want to Take Control of Their People's Data from Big Tech." *The Conversation*, 26 Sept. 2019,

theconversation.com/digital-colonialism-why-some-countries-want-to-take-control-of-their-peoples-data-from-big-tech-123048.

"International." *Electronic Frontier Foundation*, www.eff.org/issues/international.

"Internet Way of Networking Use Case: Data Localization." *Internet Society*, www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/.

Jung, Maximilian. "Digital Capitalism Is a Mine Not a Cloud | Transnational Institute." *Www.tni.org*, 21 Apr. 2023, www.tni.org/en/article/digital-capitalism-is-a-mine-not-a-cloud.

Kwet, Michael. "Digital Colonialism: US Empire and the New Imperialism in the Global South." *Race & Class*, vol. 60, no. 4, Jan. 2019, pp. 3–26, https://doi.org/10.1177/0306396818823172.

Ndemo, Bitange. "Addressing Digital Colonialism: A Path to Equitable Data Governance | UNESCO Inclusive Policy Lab." *Unesco.org*, 2020, en.unesco.org/inclusivepolicylab/analytics/addressing-digital-colonialism-path-equitable-data-governance.

OBSERVER RESEARCH FOUNDATION. "Digital Sovereignty in a Time of Conflict." *Orfonline.org*, 2026, www.orfonline.org/expert-speak/digital-sovereignty-in-a-time-of-conflict. Accessed 19 Jan. 2026.

Pinto, Renata Avila. "Digital Sovereignty or Digital Colonialism?" *Sur - International Journal on Human Rights*, 16 July 2018, sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/.