Geopolitics of technology: actors, processes, and dynamics

Sergio Maydeu-Olivares
About this report:
Title of the report: Geopolitics of technology: actors, processes, and dynamics

Author: Sergio Maydeu-Olivares

Date of publishing: March 2023

Revised by: Hernán Cortés, Carlos Bajo, Natalia Pereira

Layout by: Jimena Zuazo, Carlos Bajo

Translation in English: Daniel William Parsons

Published by the Directorate of Global Justice of the Barcelona City Council

License: Creative Commons BY-SA (Attribution Share Alike) International (v. 4.0) y GFDL (GNU Free Documentation) licenses CC BY-SA: Creative Commons Attribution Share Alike 4.0 International.

“This report has been commissioned by Oxfam Intermón, as part of the Global Digital Justice programme, promoted jointly with the Barcelona City Council. The views expressed in this publication are those of the author and do not necessarily reflect the views or opinions of Oxfam Intermón or the Barcelona City Council.”
# Table of Contents

**Introduction**

Everything has a price 3

1. From fossil fuels to stones 4
   1.1. Geography is also technology 8

2. The technological world and its geopolitical impact on the international order 10
   2.1. From the bipolar world (U.S.A. - U.S.S.R) to bipolar spheres of influence (U.S.A. - China) 10
   2.2. The pandemic and the war in Ukraine 13
   2.3. Africa in the crosshairs 15

3. Democracy, (dis)information and extremism 18
   3.1. Case study: the Rohingya 22
   3.2. Case study: the far right 23
   3.3. Case study: Cambridge Analytica and the whistleblowers 24

4. The dynamics of power in the technological era. One world, two visions, various internets? 26
   4.1. The technologies at the centre of commercial (and not so commercial) disputes 30

5. An approach to the rules of the game of the technological revolution: regulations 34

6. Conclusions and uncertainties 37
The debate about the health of democracy today is strongly linked to the analysis of the impact that technology and digitalisation have on the social contract and the distribution of power in the world. The same is true for political systems. In recent years, power dynamics have concentrated around large technology companies, a process in which governments of all political stripes have often lagged behind technological advances. First the pandemic and then the war in Ukraine have accelerated many of the geopolitical tensions in the world in recent years and technology has been a central player in the disputes: on the one hand, between states and governments, between models of digital governance and rights or among societies and, on the other hand, in key sectors like industry, business, security and defence, communications and culture. In this report we aim to provide an overview of some of the central topics when addressing the geopolitics of technology and offer some keys that will help us to better understand an ever-changing, accelerating dynamic.
Introduction

In today’s world, the fourth industrial revolution\(^1\) has placed technology at the centre of global geopolitical dynamics. We are fully immersed in a transitional process from the international order established after the end of the Second World War towards a new order that is still being established. In this new system under construction, the main players from the previous system are refusing to relinquish their hegemonic status to other parties and autocratic regimes are claiming a greater role against a kind of globalisation that has favoured the so-called global north. To better understand what kind of international order awaits us in the future, the historian Paul Kennedy\(^2\) highlighted the need to look back and detect that historically the dynamics for change, which this current technological race is, have consequences for social structures, political systems, military power, and the position of states in today’s world. These states that once led the international order, whether by seduction or imposition, which they themselves created today face the reality: several governments and private players are pushing to change the system of rules under which we have lived in recent decades, while others are resisting.

---

In this new dynamic that is still being created, the technological front, information, security, natural resources, industrialisation, energy, and the internet form part of different geopolitical disputes, yet this tension also encompasses the fields of education, healthcare, agriculture, genetics, the fight against climate change, waste management and things so mundane as going shopping and carrying out basic large- and small-scale administrative processes. This is taking place in global and in local settings, and also from the personal and specific. Technology touches (almost) everything and in the struggle to lead this fourth revolution, whether due to being well positioned in the technological race or, simply, in order to not be left behind, many countries, companies and civil society organisations are making their mark in an increasingly complex world full of uncertainties, but also of hopes and opportunities.
Geopolitics of technology: actors, processes, and dynamics

Everything has a price

While the geopolitics of now played a central role in international relations after the Second World War, today it is the geopolitics of technology that is now redefining international relations. Access to fossil fuels was historically a source of conflict and geostrategic interest in a bipolar world where the two major powers, the United States and the U.S.S.R., determined the framework of international relationships of each and every world government, as well as their societies, until the fall and collapse of the Soviet Union and the disappearance of the geopolitical block that it encompassed. The hegemony of the United States became ever present. Technologies, for example, green energy, are the replacements for fossil fuels, and access to them, in all their dimensions (resources, production, distribution, consumption), is marking the current historical period. Here is where a new technological (and energy) order is being built while some powers are calling for a change in the global geopolitical board. The exact same thing is happening with the current technological revolution. This means that geopolitical relationships are shifting not only towards countries that can provide a competitive advantage with regard to access to technology, but also towards those that possess the key natural resources to implement their technological projects. These countries are those that are home to rare metals, those that have key cutting-edge industries in the production chain of certain technological products (such as chips) and those that are relevant within the technological value chain. The progressive replacement of fossil fuels with renewable energy sources is repositioning the role of many medium-sized players. In this still unfinished and undefined process, first the pandemic, as a factor that distorted the global supply chain, and then the war in Ukraine, which has impacted the energy, economic, military and even technological field, are putting this process on hold.

In this reshuffling of the international order, technology has been fostering both international cooperation and competition. This is precisely where we have several fields to analyse and understand in order to size up the current geopolitics of technology. If we do not grasp how the technologies which are being deployed work, as well as their complexity, how they interconnect with one another and, especially, how they interact with global (and local) political, social, and economic systems, we will not be able to understand our local or global surroundings. Certain responses are causing the return of nationalism to the detriment of globalisation, the defence of private against general interests, and protectionism against the free market, in addition to the mentality of clashes and competition.

This also applies to how governments should address the adaptation of their systems to the new technological reality and of certain institutions and rules built decades ago which nervously observe how technological innovations pose a challenge for public institutions. For the last ten years there have been more objects connected to the internet than people. The acceleration and universalisation of connectivity is growing. According to estimates from the ITU, in 2021 around 4.9 billion people used the internet, which means about 63% of the world’s population. This represents a 17% increase in users, with nearly 800 million more people connected compared to 2019, especially in Africa, Asia and the Pacific and the least developed countries (LDC)³. This growing access to the internet has been accompanied by an explosion of technologies that generate and use data which are changing the markets and the way in which we relate to one another. Governments are implementing a series of measures to face the challenges involved in technology, not only for their citizens, but also for the governments’ own existence. In this context, there are increasingly more players, in particular in the business sphere, which are blazing the paths of the future in broad economic, social, and political layers.

\*\*\*

In today’s technological race the international dynamics have once again placed geography and the access and control of the land and natural resources at the centre of several geopolitical disputes and the reshuffling of industrial strategies, in particular in the fields of defence, security and the energy transition. This has led certain countries to deploy a variety of intervention strategies (in business, diplomacy, the judicial field, development policies, military support, and more). It has also generated the opposite effect, leading to increased protectionism and nationalism.
One of the elements which has turned out to be key for the development and gathering momentum of the current technological race are inner transition metals (rare metals), an essential ingredient for many of today’s technologies, vital for the energy transition, information technologies and security and defence, among other sectors whose long list includes: computers, telephones, hybrid cars, wind turbines, solar panels, medical devices, precision-guided arms, drones and more. All these products operate thanks to more than thirty critical raw materials formed by lanthanide and actinide chemical elements that have different magnetic, optical, and electronic properties. The first are those known as rare-earth elements, lanthanum, cerium, praseodymium, neodymium, promethium, samarium, europium, gadolinium, terbium, dysprosium, holmium, erbium, thulium, ytterbium, and lutetium, in addition to scandium and yttrium.4

Although there is competition for these nearly thirty rare metals, the attention is increasingly focused on the lanthanides. These are rare-earth elements. These seventeen metals are expensive and complex to extract and process. China possesses a third of the global reserves, followed by Brazil, Vietnam, and Russia5. Whoever controls the minerals controls the industry. This is true in the present and, above all, looking towards the future.

The global economy is replacing fossil fuel energy with green energy, leaving China as the primary and leading exporter of rare metals, without which technology, and the global economy would not move forward. Rare metal deposits are abundant in the world, but China has a larger proportion and variety, in particular of rare-earth elements, and the country has a short- and medium-term strategy that has made it the main country within all the technological production chains. Additionally, although China possesses the largest reserves and is the largest producer, it is also the main consumer. Its competitive advantage is evident and has allowed it to expand its sphere of technological influence, not only as a main exporter of rare metals and rare-earth elements, essential for technological production, but also as an exporter of technological products. China is committed to being a country driven by domestic consumption as well as a supplier of products and knowledge. The outsourcing of industrial and technological companies that occurred in Europe and the United States in recent decades, attracted due to China’s trade policy and its stimulus policy, as well as its extremely low business costs, has allowed China to acquire knowledge in the industrial and technological value chain that has positioned the country in the foreign market.

In this race to control rare metals and rare-earth elements, certain peripheral Latin American and African countries have a geopolitical advantage compared to other countries due to having mineral resources. The focus should not only be on extracting the elements, but also on providing value in the production chain.

China’s nearly absolute dominance of the rare metal market has been used as an element of seduction and dissuasion in its technological and geopolitical race. In 2010 China halted its exports of rare metals to Japan6 as part of a broader strategy to pressure Japan related to the claims for sovereignty over the Senkaku archipelago in the South China Sea, with the subsequent damage not only for Japan, but also for the technological supply chain of which it was a fundamental part. China not only has direct access to rare-earth elements, which are found in abundance within its borders, but it also dominates the production and access to these elements in other countries, such as cobalt mines in the Democratic Republic of the Congo. This Chinese dominance has established a geopolitics of technology linked to geography, mining resources, and states that produce and consume rare metal and rare-earth elements. The possibility of an interruption in the rare-earth element supply chain would severely impact any country’s defence and communications capacities.

---

4 Prego, R.; Las tierras raras. Los libros de la Catarata, febrero 2019
is at the forefront on this issue, forcing other powers to promote programmes not only to diversify their rare material suppliers, but also to produce these elements. One of the direct consequences is the resurgence of mining nationalism across the world in recent years, both in countries that boast active rare-earth and other metal mines of strategic value and in other countries that closed a good part of their mines in the 1980s and 1990s and relocated them to other countries, and which are now considering reopening or returning to mining (Sweden and France, most recently).

This geopolitical instrumentalisation of natural resources, energy, food, technology and other raw materials has been a constant in recent world history. It is not an isolated phenomenon; on the contrary, it is commonplace. We can find some of these examples in OPEC’s decision in 1973 to increase the price per barrel of oil, ordering cutbacks in production and a total embargo on the United States and the Netherlands due to the West’s support of Israel during the Yom Kippur War, during the United States’ grain and technology embargo in 1980 on the U.S.S.R. due to its military support to Afghan communists and, more recently, Russia’s shutting off the gas tap to Europe as a reprisal for European embargoes due to the war in Ukraine.

Accustomed to using all types of technological tools, a good part of citizens are unaware of which components are necessary to manufacture technological devices, nor of where and how they are obtained, nor of the price which has been paid for them, both in terms of human rights as well as in environmental impact. Additionally, the high level of dependency on China and the trade war between China and the U.S. is pushing many states, in both the global north and south, to restart a mining race to ensure a certain degree of rare metal independence or, at least, to gain a competitive advantage that allows the countries to exchange resources for their own benefit and to diversify the suppliers who provide these materials.

This activity is accompanied by an ethical debate linked with the mining industry itself, the technology industry that makes use of it, the responsibility of civil society that makes use of technological advances, and the energy transition policies promoted governments around the world. As Piltron notes, if the mining industry that other parties such as China and African countries produce, from which we benefit, has an unsustainable environmental impact based on the western viewpoint, the reopening of mines on European soil would be the best environmental decision possible to be able to reduce the environmental footprint caused by accessing rare metals, ensuring that the mining operations model is suited to European environmental standards. The technostrategic race for rare metals is full of contradictions, as extraction and processing are linked to a major environmental footprint. The environmental cost of the energy transition, and of the entire technological value chain, should also be borne in its entirety by European citizens.

In the current geotechnological dispute, the United States is in an inferior position in the rivalry with its main competitor, China. This struggle is marked by a constant fear of a reduction or embargo on the export of rare metals by Beijing as a reprisal due to the anti-Chinese technology policies adopted by both the Trump and Biden Administrations. The U.S. is dependent on China’s rare-earth elements for nearly 80% of its needs. An interruption in the value chain is a serious threat for American tech giants, whose technological production chain would clearly be affected.

---

Meanwhile, the European Union has a much greater external dependency on China for rare-earth elements, accounting for 98% of the EU’s needs, according to data from the European Commission\textsuperscript{10}, although sites have been found in Sweden, Finland, Greece, and Spain that could help the EU to reduce its dependency on Beijing in strategic sectors, though this would not happen in the short term. The identification of deposits has advanced in recent years with public-private partnerships. The challenge that both EU authorities and national governments are facing is how to extract and process them with the minimum environmental impact possible, while guaranteeing their profitability. Spain is one of the first countries to address this, publishing a sustainable raw materials management guide, in which the country commits to “a more sustainable, circular, safe and efficient mining activity”\textsuperscript{11} linked to strategic autonomy and the energy transition, a strategy in which Spain has positioned itself as an international leader. The energy security and ecological transition related to rare-earth elements are a matter of national security for Spain, as was reflected in the latest strategy published in 2021\textsuperscript{12}.

The fact that the United States, China, the European Union and Russia\textsuperscript{13}, four of the world’s premier arms powers, are vying for access to, control over and production of rare-earth elements also fits within the logic of a clear competition in the race for the use of technology for military purposes. Without rare metals and rare-earth elements there would be no night vision devices, radars, precision guided arms systems, navigation systems, batteries, latest generation fighter planes, drones, or communications satellites. Magnets, of great strategic value in the military field, whether they are made of samarium and cobalt or with neodymium and iron, are currently one of the causes of major concern for the security and defence of the United States and several European countries, although this is also true for Russia, given that magnet production depends to a great extent on China.

The implications for their respective security and defence industries, in the midst of an accelerating arms race due to the war in Ukraine, and for their own national security are evident.

One of the greatest risks associated with this technological race is that the independence from fossil fuels linked to the energy transition that we are heading towards is giving way to a (problematic) dependence on rare metals and rare-earth elements.
1.1. Geography is also technology

The fight over the land in this phase of today’s geopolitics of technology is also being settled in specific geographic areas, such as continental shelves and the Arctic, including not only resources linked to rare metals, but also to fossil fuels.

In recent years the Ivory Coast, Papua New Guinea, China, the Philippines, Morocco, the United Kingdom, Spain, Norway, Chile, Argentina, Portugal, Libya, Turkey, and a long list of other countries have had or are having contentious diplomatic relations for the delimitation, if not expansion, of their exclusive economic zones (EEZ) and their continental shelves. The delimitation of new maritime borders and, therefore, gaining sovereignty over their waters is opening new geopolitical disputes. Sovereignty over waters also includes the sea beds, the subsoil and all the scientific, technical, and mining interests that derive from them. Mineral findings on land are subject to increasingly greater pressure. The seabed is the great hope for the development of underwater mining. Meanwhile, environmental groups are warning about the enormous risks that implementing this kind of mining would have on marine biodiversity14.

In this race for continental shelves, the United States signed a memorandum of understanding in September 2022 with the Pacific Islands15, whose territories are facing strong pressure from the Chinese expansionist policy throughout the Pacific which is claiming the territory of large continental shelves linked to the creation of artificial islands. Through this agreement, the United States will provide financial assistance to promote agricultural development projects in matters of security and technology, the protection of the fishing sector and marine protection16. This pact is linked in turn with the approval of the first Indo-Pacific Strategy17, in which the geopolitics of technology are notably present.

As for the Arctic, calculations show that 30% of the undiscovered gas in the world and 13% of undiscovered oil can be found in this region18. In recent years, several countries have started a geopolitical dispute in this area. The thawing of the Arctic caused by climate change will change the current rules of the game in the field of international trade by opening new routes as well as in the energy market and in the access to rare-earth minerals and metals. This growing rivalry is reflected in the Arctic Council, a forum for regional cooperation that includes countries that border the Arctic such as Russia, the United States, Finland, and Canada, and also features observer member countries such as China, Spain, Italy, Germany, Japan, India, and the United Kingdom. For the smaller member countries, such as Iceland, Finland, Norway, Sweden, and Denmark, which form the backbone of the Arctic Council, this council has evident geopolitical implications. The Arctic Council is becoming another technodiplomatic space of dispute between major powers.

14 Ecologistas en Acción. Informe “Ojos que no ven… La minería submarina en España”. July 2020
15 This includes the governments of the Cook Islands, the Federated States of Micronesia, Fiji, French Polynesia, Nauru, New Caledonia, Palau, Papua New Guinea, the Republic of the Marshall Islands, Samoa, the Solomon Islands, Tonga, Tuvalu, and Vanuatu.
16 Edel, Ch.; Poling, G.; Johnstone, C.; White House unveils Pacific Islands strategy at historic summit. CSIS, 30 September 2022
https://www.csis.org/analysis/white-house-unveils-pacific-islands-strategy-historic-summit
17 White House. Indo-Pacific Strategy. February 2022
https://pubs.er.usgs.gov/publication/70035000
China drafted its first “Arctic Policy” in 2018 setting out its priorities in the region, despite not having a border with it. This strategy forms part of the “New Silk Road”, of the polar silk road, which has led it to establish partnerships and investments with countries and territories that have an Arctic border such as Norway, Iceland, and Greenland. The United States considers this strategy a threat to its national security. This dispute for the control of the Arctic also involves Russia, which considers “some countries’ attempts to revise provisions of international treaties regulating economic and other activities in the Arctic and establish national regulation systems without taking into account regional and international formats of cooperation”, in reference, for example, to Norway and the United States. Russia’s political stance, like that of its rivals, is for the Arctic to continue being a “region of peace”, though its policies show otherwise. Putin’s government has increasingly higher levels of interest in the region. This is due to the promotion of socio-economic development plans on fossil resources, the geological exploration of rare metals and, in terms of trade, the creation of the North Sea Route. The United States has not lagged behind. At the end of 2022 the country published its strategy for the Arctic which, on paper, is committed to working in the region based on four pillars: security, environmental protection and climate change, sustainable economic development, and international cooperation and governance.

---


2. THE TECHNOLOGICAL WORLD AND ITS GEOPOLITICAL IMPACT ON THE INTERNATIONAL ORDER

2.1. From the bipolar world (United States - U.S.S.R.) to bipolar spheres of influence (United States - China)

In order to understand today’s world, we need to take a look at the past. The current international order was built 80 years ago as a consequence of a war and resulted in two political, economic, and social models led by the United States and the U.S.S.R. squaring off in opposition to each other. During those decades, the technological race was spearheaded by the space race and the arms race between the two countries and their areas of influence, which served as the driver for military technology development until today in a wide range of fields, from communications to pharmaceuticals, from the labour market to the agricultural and fishing sector, from transport and mobility to energy and industry. The breakup of the U.S.S.R. in the 1990s led to a unipolar world led by the United States and the start of an era of optimism in the West, but also one where other countries started to question that leadership which was never complete or definitive. The start of the 21st century completely burst the many people’s bubbles of optimism and universalised the reality of others.
This bipolar world has turned into a multipolar one. The United States continues to have a leading role with China as its main competitor, which has taken up an increasingly central role in international dynamics. While the United States in recent decades was enmeshed in multiple military fronts abroad in the midst of an international financial crisis, China rapidly increased its economic power, military strength, and global political influence. Here is where technology and China are fighting another battle.

According to the United States Government, the Chinese Government aims to steal western technology, a situation that would give Chinese companies a vital economic and competitive advantage. For China, the United States does not want to relinquish its hegemonic role in international dynamics. For the United States, China is its main strategic competitor and technologies are one of the central elements of this division that is dragging in many countries which are also dependent on the resources and technologies of these two nations. For China, the policies of the Trump and Biden Administrations, which have restricted access by Chinese companies to the American market and to American technology, have been seen as an attack on China's sovereignty and its renewed role as a leader in global trade.

Both the United States and China have been immersed in a trade and technological war for years which is leading to the establishment of technological spheres of influence. Both countries are seeking to establish the pre-eminence of their respective technological models over other countries, reinforcing old alliances, or seeking out new ones, above all, ones in which there is no room for alliances with the leader from of other sphere. From absorption to exclusion. In the meantime, many countries and players are trying to create a mixed technological environment. While Thailand is strongly dependent on Chinese technology, Japan has done everything possible to avoid that fate, wagering not only on its own technological capacities, but also aligning itself with the technology of its greatest ally, the United States. However, the technological chain has few airtight spaces, which makes it difficult to create exclusive technological spheres. Despite the efforts of various countries to create exclusive areas, technological interdependence does not allow for decoupling, at least not for now.

The configuration of these spheres of technological influence is the natural result of this geopolitical rivalry in the technology field, where the United States and China are struggling to create spaces of dominance or control over the technological arrangement and where we see a third player, the European Union, trying to forge its own path aware of its own limitations and dependencies. While the Chinese model advocates for placing the State at the centre of technological governance, the American model places companies and other state actors at the centre.

Technology is a tool of a model of influence, of understanding international relations, of social and political construction, and of a vision of human and digital rights that goes beyond the merely industrial. The growing rivalry between the United States and China is shaping a structure of technological governance with the goal of exerting a predominant influence.
We can find one of the resulting unions in this technological and geopolitical race and rivalry in Russia and China, which in recent years have cooperated closely, starting with the call for a new multipolar international order, questioning the primacy of the United States, which goes beyond even classical geopolitics. That is why the two powers have been increasing the number of joint declarations and agreements in recent years and they are vital in order to understand the technological dynamics between governments and technological spheres, which are a central space in the current geopolitical tensions\textsuperscript{24}.

The relevance of this alliance also lies in promoting a vision of democracy and human and digital rights that is far removed from the prevailing international standards to date. In fact, it is linked to a different relationship with the United Nations Charter signed in 1945. They state verbatim “There is no one-size-fits-all template to guide countries in establishing democracy. A nation can choose such forms and methods of implementing democracy that would best suit its particular state”\textsuperscript{25}. This joint declaration highlights an alliance between the two countries based on the geopolitics of technology as well, which ranges from artificial intelligence to information security, and security and defence. The two governments cooperate closely in this field, both in the rare metals market and in the fossil fuel market, and in the commitment to forge a new model of internet governance that defends their interests, where it is the state who determines them.

In the geopolitical field, the joint Russian-Chinese commitment also includes greater coordination with the rest of the BRICS countries\textsuperscript{26}, a space for cooperation between Brazil, Russia, India, China, and South Africa. At the moment, this technological coordination among the BRICS is more a declaration of Russian-Chinese intentions than a reality. Russia and China seek to expand this cooperation to other countries, such as Saudi Arabia. This is due to the need to define their own spheres of influence and to make them effective, including countries with added value in the technological, energy, geostrategic or political field, thereby expanding their capacity for global influence.

\textsuperscript{24} This call for a new order was reflected at the start of 2022 in the following joint statement: “Certain States’ attempts to impose their own ‘democratic standards’ on other countries, to monopolize the right to assess the level of compliance with democratic criteria, to draw dividing lines based on the grounds of Ideology, including by establishing exclusive blocs and alliances of convenience, prove to be nothing but flouting of democracy and go against the spirit and true values of democracy. (…) The sides call for the establishment of a new kind of relationship between world powers on the basis of mutual respect, peaceful coexistence and mutually beneficial cooperation”. Source. Joint Statement of the Russian Federation and the People’s Republic of China on the International Relations Entering a New Era and the Global Sustainable Development. 4 February 2022 URL: http://en.kremlin.ru/supplement/5770


2.2. The pandemic and the war in Ukraine

Two globally disruptive events that happened in the last three years, the pandemic and the war in Ukraine, mark the current geopolitics of technology and have led to an immediate reaction from governments all around the world. This has kicked off a race for strategic self-sufficiency that encompasses several fields: food, energy, healthcare, technology, and more.

The COVID-19 pandemic was the first major collective challenge that humanity has had to face in decades. It revealed the inability of many governments to address the management of the pandemic starting from the most basic elements, the lack of healthcare products, and their major foreign dependency. In the technology field the pandemic gave countries the opportunity to tackle existing challenges and be prepared for future ones by harnessing and leveraging technology. Part of the public health response to the pandemic led governments around the world to promote technological programmes to track, trace and locate citizens. Singapore, South Korea, Switzerland, Ireland, Spain, and China were some of the countries that set up tracing strategies with varying degrees of success. The development of any healthcare application involves a wide array of technical and practical challenges, including those related to human rights and cybersecurity. While some countries gave primacy to control over rights (China), others tried to find balance in the midst of the crisis, which led to a poor crisis management and minimal results (Europe). Specifically, China made use of positioning technologies to track patients and impose lockdowns and other restrictions with its “Zero COVID” policy, repeatedly placing cities and regions under quarantine. China became a surveillance State, with cybernetic social control capacities over the population, based on the deployment of a large number of surveillance systems from drones to closed circuit television cameras, as well geospatial information in mobile applications like WeChat and Alipay, tracking people’s locations and identifying at-risk individuals through cross-referencing. In parallel to this technological deployment, China’s health surveillance system utilises a wide network of governmental institutions and civil platforms that complement the surveillance network outside the technological sphere. These involve residents’ or villagers’ committees to give two examples. This experience has allowed the Government of Xi Jinping to further strengthen a technopolitical model based on censorship, propaganda, and surveillance.

Compared to the European model that prioritised rights and privacy, opting for other healthcare management models, China's case has served so that many authoritarian and autocratic regimes can draw lessons on how to improve, use and apply restrictive technologies as social control over the population. The continued use of these technologies continues to be an imminent concern for the international democratic community due to the implications it has on civil liberties.

---

Far from the technological advances and the trials that occurred to manage the pandemic, including pharmaceutical advances, the pandemic also led to a technological revolution insofar as companies and governments had to reinvent themselves, incorporating digital technology in the labour market and accelerating global supply chain processes. The digital divide here clearly showed the strengths and weaknesses of many countries and companies and spurred a race for technological adaptation, at the risk of being left behind. The educational sector stood out in this process, which had to adapt at full speed to guarantee access to education for millions of children around the world. This goal was not always achieved31. The pandemic had a major impact on the global educational system and led first to confirming the existing digital divide, not only between countries, but also within them. In the EU, the rapid acceleration in digitalisation in European countries brought with it, for example, questions about the role that technological companies and digital educational platforms might have concerning the rights of children32.

The second disruptive factor in recent years, the war in Ukraine, is having a direct impact on the current and future relationships between the European Union and China on technology matters and with other countries on matters of energy, food security, and security and defence. In the words of the president of the European Commission after the European Council of 21 October 2022, “we have learnt our lesson concerning the over-dependency on fossil fuels from Russia, and how tough but necessary it is to get rid of this dependency.” This Council meeting once again put forward the issue of the EU’s dependency on China for technology and raw materials along with the need to reinforce strategic autonomy, as well as the diversification of raw material suppliers, including rare metals, which are essential for technological development33. In 2021, the EU identified 137 highly sensitive products that it imported, of which 99 were products related to raw materials and chemical products, and which made it especially dependent on other countries, including China, Vietnam, and Brazil34, thereby affecting European technological autonomy.

We recently saw how, due to the war in Ukraine, Facebook, and Instagram politically positioned themselves by announcing35 that they would allow posts that urge violence against Russia. One of the largest tech companies (both platforms belong to Meta) chose a side in a geopolitical conflict. We have seen some examples in this report about the role that technologies play in today’s geopolitics, but this specific case is not just another in this analysis as the war in Ukraine is a good example of interventionist practice by foreign tech companies. Another example is Starlink, a company led by Elon Musk, which with the deployment of its satellite system36 is enabling operability and internet access in Ukraine in the midst of the war. Without Starlink Ukrainian troops would have found it difficult to maintain fluid communications among themselves, especially after the Russian army destroyed practically all of the Ukrainian communications systems and many critical energy infrastructures.

34 European Commission. Strategic dependencies and capacities. Updating the 2020 New Industrial Strategy: Building a stronger Single Market for Europe’s recovery. 5 May 2021
36 Musk, E. @elonmusk). 26 February 2022 “Starlink service is now active in Ukraine. More terminals en route”. Twitter https://twitter.com/elonmusk/status/1497701484003213317
The pandemic and the war in Ukraine, both events with an international impact, have been an accelerant leading to many other countries, also from the global south, striving for greater national and/or regional strategic autonomy. The drive to set up the African Continental Free Trade Area and other viewpoints from Latin America are a good example of this.

In the corporate field the role that certain tech companies have in the development of the war stands out. We have already mentioned the role of Starlink in maintaining Ukraine’s communications during the war, but we could mention that Facebook, Twitter, and other media companies have restricted access to Russian media in the EU following the guidelines of the Council of the European Union after European and United States government authorities had accused these Russian outlets of disinformation.

With the war, the European Union has opened another front concerning the security of critical infrastructures, especially energy and technology infrastructure. Strategic autonomy in times of pandemic and war. The European Parliament recently published a report on the security of technology cables indicating the need to reinforce their security and highlighted not only the importance of this type of infrastructure for global internet traffic, but also the threats that loom over them, especially in international areas removed from the territorial control of states. From the European standpoint, two of these threats were Russia and China. Concerning the latter, the report expressly mentioned how China has gained momentum in recent years and cited the threat that it poses in data interception and the technological dependency that had been created.

2.3. Africa in the crosshairs

One area of technological interest that the war in Ukraine has once again highlighted is Africa, one of the traditional regions of dispute by major powers and global economic players. Not only is Africa a historically key strategic region in the formation of spheres of political and economic influence, but it is also a source of natural resources, in particular mining resources, which has attracted the interest of foreign countries to the detriment of national interests, in particular the interests of their populations.

Russia has a long-standing interest in the continent, although it has become more acute in recent years. Russia’s main strategic goals in Africa are clear: to expand its geostrategic presence and broaden its area of influence to confront the West and to establish a source of key natural resources for its technological race. In exchange, Russia offers support in key security matters in today’s world, against the advance of jihadism in a variety of African countries, against the political and social instability and increased insecurity, and business agreements and investments in sectors like energy, minerals, grains, and hydrocarbons.

---

In 2019 the Russia–Africa Summit prompted agreements between Russia and several African countries\(^{42}\). The declaration itself highlighted the need to cooperate, for example, on matters of energy security, on renewable energies and on joint technological projects and also on matters of information technologies security. In terms of security and defence, the Russian government has signed agreements with more than thirty African countries.

A few months after hosting this summit, the Stanford Internet Observatory\(^{43}\) and Facebook denounced a disinformation and electoral interference campaign that had the support of Russian cyber networks in several African countries, including the Central African Republic, Sudan, the Democratic Republic of the Congo, Madagascar, and Libya. Thanks to the use of Russian cyber warfare applications and political technologies and with campaigns on social media, the Russian government has established the grounds to create a favourable environment in the long term for Russia’s interests in Africa. We were able to see this in the first stages of the war in Ukraine at the United Nations General Assembly headquarters. On 2 March 2022 seventeen African governments voted against or abstained from the resolution that condemned Russia’s military intervention in Ukraine.

In terms of security and defence, Russia’s assistance to several African governments\(^{44}\) has been on the rise: from military assistance and arms purchases —for example, from Nigeria and Egypt— to advising on political and social disinformation campaigns and shutting down or interrupting social media. The presence of the Wagner mercenary group\(^{45}\) in Africa has significantly grown in recent years: Sudan, Mali, Libya, and the Central African Republic. However, the presence of foreign international security companies is not exclusive to Russia. Sadat, a Turkish security company, supports the state armies in Ethiopia, Somalia, Sudan, and Libya\(^{46}\). Turkey’s geostrategic interests in Africa have also been increasing. The need to find new markets for the development of the Turkish technological industry is also a priority for Erdogan’s Government.

The reaction of Europe and the United States to the movements of their two main geopolitical rivals, Russia and China, in recent years has been relatively rapid. In the case of the European Union\(^{47}\), it is striving to establish a specific policy of development and cooperation in Africa\(^{48}\) which includes an investment package of billions of euros in matters of energy, transport and digital infrastructure, the environmental transition, the digital transformation, and policies that promote a fair energy transition. This road map to collaborate with the continent on promoting the digital transformation in Sub-Saharan Africa\(^{49}\) is taking place in parallel to a revision of European participation in matters of security and defence, especially against the jihadist threat that operates in vast spaces of Sub-Saharan Africa and to address irregular immigration in the region, which is also considered a problem for European security. On immigration policies, there is a concern in Europe due to the impact of the transfer of surveillance capacities\(^{50}\), including technological capacities, that European projects deploy especially in the Sahel together with African governments.


While China’s operations in Africa are aimed at setting up the borders of today’s geopolitics of technology that take shape in the Digital Silk Road, the United States is doing the same through the Build Back Better World initiative51, promoted through the G7, while the European Union is promoting its Global Gateway52.

Recent Western political movements that have a renewed commitment to the continent highlight how China's growing economic presence in Africa, especially in the technological and digital fields53, has unleashed a geostrategic competition that works in the continent’s favour54. This competition also includes medium-sized players, such as Turkey, which has opened 26 new embassies on the continent in only 5 years, as well as Brazil, Saudi Arabia, and the United Arab Emirates. Turkey became a strategic partner for the African Union in 200855. Africa is not only a continent with abundant natural resources required for the energy transition, but also a point of instability for the European Union, for example, in matters of migration and security, and votes in the United Nations General Assembly and the Security Council in the dispute over the establishment of a new world order. Africa is also in full political turmoil, which has led to democratic backsliding for some countries in the region, especially in the Sahel. Today Africa is a disputed border for the major global powers, where the technological war in particular takes on a central role with the goal of obtaining more natural resources and a greater presence of foreign companies.

But this interest in Africa within the geopolitics of technology starts, in particular, with the African countries themselves. In 2015, the African Union promoted the Agenda 206356, a strategic concept for Africa's socio-economic transformation by 2063. This agenda includes fifteen flagship projects: cybersecurity, space technology, a Pan-African digital data network and online services, transport, renewable energies, and open and digital education. In terms of raw materials from fossil fuels to rare metals, these projects mean that Africa will cease to be a continent that supplies resources in order to become a supplier of products that drive greater technological sovereignty. This requires external support. China, Russia, the United States, the European Union, Japan, Turkey, and Brazil are running in this race. Ceasing to be a supplier of resources in order to become a supplier of products is not a desire exclusive to African governments. All the governments that have entered the race for rare metals and the revitalisation of the mining industry, a requisite to be in the technological race, aspire to this same goal.

51  White House. “President Biden and G7 Leaders Launch Build Back Better World (B3W) Partnership” https://www.white-house.gov/briefing-room/statements-releases/2021/06/12/fact-sheet-president-biden-and-g7-leaders-launch-build-back-better-world-b3w-partnership/
The rapid advance of information and communications technologies has had a profound impact on democracies across the world. They have provided new platforms for civic mobilisation and for spreading news and comments, but are also subject to censorship, surveillance, and exploitation by anti-democratic forces. They have also represented a revolution in restrictive political and social environments, providing players who traditionally have merely received messages the opportunity to also send messages, which has made it easier to contest the one-way messaging from authoritarian governments and authorities. This greater capacity to access information has in turn enabled greater democratisation of information and also the opposite, the need by certain political players to restrict access to information and sending messages and to enhance their control over information. Digital communications technology has more importance in geopolitics, as we were able to see during the Arab Spring and in the hybrid war promoted after the Russian invasion of Ukraine and during the pandemic, where technological surveillance highlighted the desire of certain governments to control the population. As Mounk states, “digital technology destabilises government elites from around the world and accelerates the pace of change”\(^{57}\).

---

57 Mounk, Y. *El pueblo contra la democracia. Por qué nuestra libertad está en peligro y cómo salvarla*. Barcelona: Editorial Paidós, 2018, page 154
Disinformation is not a new phenomenon. Controlling the narrative of what is truth and what is a lie is nothing new either. It is part of the history of humanity. However, technology and social media have facilitated the spread and therefore the scope of disinformation. This terrain is ripe for extremism to have a bigger mouthpiece than it had, such as the cinema and the press in Nazi Germany in the 1930s and radios in the 1990s in Rwanda and Burundi. In recent years examples abound of (mis)use of social media to spread hate speech and disinformation. For Mounk, “in authoritarian countries, the democratic opposition now has many more tools to bring down a dictator, but for that same reason, it is much easier for hateful demagogues to undermine the foundations of liberal democracies”\textsuperscript{58}.

The recent pandemic has been no exception. Several governments mobilised to introduce legislation against disinformation, fed by anti-vaccine groups, outspoken political leaders, the media, and radical and extremist groups. The internet amplified anti-science messages at a time when science too had many questions and not enough answers. The decision of those governments to tackle healthcare disinformation led to concerns about how these same tactics could possibly be used to limit freedom of expression and the press, prompting new regulations, which led to criticisms about how the governments were handling the crisis.

The European Union has been one of the global players that has most prioritised the fight against disinformation in recent years, in particular against disinformation coming from Russia. In 2015 the EU recognised foreign information and Russian disinformation as threats to security. Since then, the EU has been developing different initiatives with the support of other countries and civil society organisations\textsuperscript{59}, notably including EuvsDisinfo, where they identified and moved to counter Russia’s disinformation operations throughout Europe. They also attempted to address disinformation over the same period regarding the pandemic. The geopolitics of technology plays out in cyberspace.

Other governments took advantage of the healthcare crisis to limit freedom of expression, the press, and citizens’ digital rights. The former UN High Commissioner for Human Rights, Michelle Bachelet, criticised the governments of China, India, the Philippines, Thailand, India, and Myanmar, among others, for using emergency legislation that involved a clear curtailment of digital rights\textsuperscript{60}. The Council of Europe also denounced the situation in Turkey and Hungary, while in Russia the police arrested protesting politicians and citizens, using the public health restrictions imposed to clamp down on freedom of assembly. However, China has represented one of the most extreme cases, where all the digital spaces have been securitised.

Disinformation campaigns were not removed from geopolitical disputes between countries. China, Russia, and Iran have been repeatedly accused of promoting mass disinformation campaigns linked to the coronavirus\textsuperscript{61}, but we do not have to go to China or Russia to find disinformation campaigns about the pandemic. Examples abound in the United States, Latin America, and Europe, including those spread by certain national political leaders, not only about the disease itself and how to address it, but also its origin, as well as by far-right groups with the goal of undermining democracy. The WHO responded by promoting a strong digital information and awareness\textsuperscript{62} campaign about COVID with information updated daily about the advances in the global fight against COVID, research, vaccines, strategies,

\textsuperscript{58} Mounk, Y.; Idem, p. 152
\textsuperscript{62} WHO, informative website about COVID https://www.who.int/emergencies/diseases/novel-coronavirus-2019
situation reports, and more. The geopolitics of vaccines were at stake and technological advances were humanity’s best hope to deal with the greatest health crisis in the last 100 years.

Technology companies had a leading role during the pandemic, especially in the first months as the infodemic spread online. Many governments, international institutions and relevant players from civil society pressed the leading tech companies to adjust their technology policies as the infodemic spread online. We saw this role of tech companies as central players in the management of (dis)information in the United States to partially block the spread of conspiracy theories and to confront denialist campaigns online.

Beyond the pandemic we can find countless topics that have found the perfect echo chamber on social media so that all types of messages can reach any part of the world, affecting the international and domestic public debate. Social media have made it possible for senders and recipients to break down a barrier that for years had been monopolised by traditional media, the so-called fourth estate, just as for centuries the printing press and those who had access to it had been. Social media (Twitter, Facebook, and WhatsApp, to give some examples) are where extremist groups and radical ideologies have found the perfect platform to reach every corner of the world. We have all become individuals who send and receive messages.

In democratic environments, some digital platforms have restricted or prevented radical groups and individuals in particular from further hate speech. The structural conditions of communications have been transformed thanks to digital technology, which has promoted the spread of these types of messages. Twitter’s decision to close the account of then President Donald Trump is the best-known example in the field of technodiplomacy. The story on the war beyond the United States and China has also been important, with the pandemic serving as another front. For months Trump always spoke of the Chinese virus, not about COVID, linking the global healthcare crisis to China, which led to an increase in racist anti-Asian messages on Twitter.

Sympathetic media and extremist groups did the dirty work, serving as a mouthpiece for that message. The WHO responded by stressing the importance of using neutral language when naming diseases and other threats to public health. We have other known cases, for example, in the use that international terrorist organisations like Daesh made of western social media to start a propaganda campaign and spread hate speech with the added goal of recruiting sympathisers who joined its cause in Syria and abroad.

In 2019 the researchers Alina Polyakova and Chris Meserole described the use of technological capacities by authoritarian regimes to monitor, manipulate and extend their repression as digital authoritarianism. This includes the manipulation of social media and the use of artificial intelligence and other surveillance systems as tools to control internal political and social debate, while also influencing external public debates, in particular during elections. Their analysis focused on how the Chinese and Russian models of digital authoritarianism are being exported and embraced by governments around the world.

63 Definition from the Pan American Health Organization: “A massive infodemic: an overabundance of information – some accurate and some not – that makes it hard for people to find trustworthy sources and reliable guidance when they need it” - https://iris.paho.org/bitstream/handle/10665.2/52052/Factsheet-infodemic_eng.pdf?sequence=16
However, just as social media and technology have been accused of deteriorating not only public debate, but also of being a key factor in the decline of certain democracies (the United States and Brazil recently), they have also been seen as an essential element to bring civil society closer to decision making and promoting digital communications in environments where freedom of expression and other fundamental rights were restricted and limited. In recent years in Africa, we have witnessed significant democratic advances and backsliding, which have put the international community on alert. The same is also true in the digital field. Over the last three years there have been five military coups on the continent. Democracy has moved forward in Gambia, Zambia and Niger and has had setbacks in Mali, Chad, Guinea, Sudan, Burkina Faso, the Ivory Coast, Uganda, Tanzania, and Benin. In the same way that social media and information technologies have been a true revolution in the global sphere, in recent years in Africa, where the digital divide remains vast, the use of these technologies has made it possible for the younger generation and beyond to enhance their political participation. While in Uganda, Nigeria and Ghana information technologies have promoted the democratic demands of civil society in fragile environments, these governments have used them to defend their grip on power. One of the best-known cases is Uganda, where the opposition leader Bobi Wine used social media to promote his candidacy. His objective was to win the 2021 presidential elections and put an end to Museveni’s government that has been in power since 1996. Museveni’s response was immediate; he shut down internet access. From digital democracy to digital repression.

According to the latest report from Freedom House, global internet freedom has decreased for the 12th consecutive year and, in at least 53 countries, users face legal repercussions for expressing their opinions online. Digital authoritarianism has become the norm in China, Uganda, Myanmar, Sudan, Turkey, Russia, Thailand, and Nicaragua. This phenomenon is increasingly easy to replicate and export.

In parallel, the creation of spheres of technological influence has led certain companies to use technology, the internet, and information to extend their presence or to tilt existing balances to swing the balance in their favour. For example, there is strong evidence of Russia interfering in the electoral processes in Europe, the United States, Africa, and the post-Soviet space in recent years through cyber-attacks, disinformation campaigns online, the presence of mercenaries and/or the capture of political elites. The list is extensive:

68 Cheeseman, N.; ¿En qué estado se encuentra la democracia africana 30 años después?. Revista Ideas. Núm. 56
71 Babatunde, G.; Internet shutdown Uganda Technet, January 2021 https://technext.ng/2021/01/16/social-media-round-up-internetshutdownugandabobi-wine-bussitchallenge-and-other-trending-stories/
Georgia, the United States, France, Hungary, Ukraine, the United Kingdom, Spain, Libya, Germany, Zimbabwe, Poland, Finland, Central African Republic, and more.

But this increased digital authoritarianism has also had consequences on other fronts, such as on immigration issues and on defending diversity. Anti-immigration speech has been on the rise in recent years, inundating social media with hateful messages promoted by radical and far right groups. The geopolitical reality in recent years has been marked by a significant increase in forcibly displaced people around the world, especially in Latin America, Africa, the United States, and Europe, the result of conflicts and security crises, lingering humanitarian crises, climate change, and increased inequalities. These involve intrastate, regional, and international forcible displacements. In some cases, they are also the result of geopolitical games. In the digital field we have seen an increase in hate speech, which has caused an increase of xenophobic and racist attacks against the immigrant population, and in the geopolitical field this has also led to an increase in tensions between various countries: Venezuela-Colombia-Chile, Central America-United States, Spain-Morocco, Germany-Turkey, South Africa-Zimbabwe, and so on. The digital battle over the narrative has had its influence and response in the diplomatic and political arena.

In the field of citizen security, technological innovations have enabled undeniable advances in the fight against crime, organised crime, and transnational crime. In democratic environments, these synergies have brought about important debates associated with the presumption of innocence, stigmatisation, technological surveillance, prevention policies, privacy, and algorithmic bias.

3.1. CASE STUDY: THE ROHINGYA

In February 2018 the United Nations Human Rights Council published an investigation in which it accused Myanmar’s regime of “attempted genocide” against the Rohingya minority in the state of Rakhine. Hundreds of people died and were imprisoned and more than 750,000 fled to neighbouring Bangladesh in barely a year, which caused one of the world’s largest humanitarian crises in recent years. The UN Report accused Myanmar’s government of allowing and fanning hate speech through social media with the goal of “destroying, in whole or in part, a national, ethnic, racial or religious group”. For months, actors linked to the army and radical nationalist Buddhist groups used social media to start a mass campaign of hate speech and violence directed against the Rohingyas. Subsequently, Amnesty International published an investigation in which it denounced the role that Facebook had played by acting as an echo chamber for hate speech that led to a disinformation campaign with fatal consequences.
In 2021 a coup d’état brought a military regime back to power, ending the democratic transition that had started in 2011. This coup once again put Facebook in the international (and digital) media’s spotlight. After the lesson from 2017 and the 2018 United Nations Report, Facebook acted immediately and announced the closure of thousands of accounts, restricting access to members of the military government and radical political and social actors. Despite this reaction, Global Witness reported in 2021 serious shortcomings in this strategy, which did not prevent a new campaign of hate and disinformation in Myanmar.

3.2. CASE STUDY: THE FAR RIGHT

For several years in the global north, the resurgence of the far right has been considered a high-level security threat with attacks against minorities and refugees, online disinformation, intimidation, vandalism, and more. Their discourses are focused on rhetoric against immigration, promoting nativism, denying climate change, rejecting traditional politics and, more recently, the pandemic. The European Union itself has decided to address this threat by noting that the far right “spreads hate speech, promotes the dehumanisation of the target groups and incites others to use violence”. Social media plays a fundamental role in the spread of their messages.

During the early months of the pandemic far right groups, not only in the global north, exponentially increased their anti-vaccine messages as well as messages against some of the measures passed by many governments around the world, from the use of masks to total or partial curfews, remote work, and so on. They also targeted the Asian population, with whom the far right associated the origin of the disease. The implications for public health have been evident, as well as for the political and social stability of many countries, already under great stress following the initial deployment of measures considered harmful by these groups.

The use of simplistic narratives, with no scientific basis, has found notable acceptance in several countries, both in the global north and in the global south, and a considerable number of protests have happened against the decisions adopted by European, Latin American, and U.S. governments. The use of online communications has been essential for the spread of many of these theories, leveraging the lack of information in the face of a healthcare crisis for which there were initially no vaccines or effective healthcare measures, as well as the restrictions of movement themselves that facilitated online communication.

We can find an example of this in the United States, with QAnon, a group identified as a terrorist threat by the FBI, which for years has fanned different conspiracy theories and which started a campaign of mass disinformation online with the pandemic. Some of the messages were amplified by President Donald Trump during the last stage of his presidency.

---

But the disinformation campaigns from far-right groups have also been linked, for example, to 5G technology92 or the role that Bill Gates and the philanthropist George Soros have had both in the origin and the spread of COVID-19. Disinformation campaigns widely spread by other states. In recent years, politicians from Italy, France, and India, for example, have also been spokespersons for these campaigns. In the age of social media, the speed with which conspiracy theories and disinformation spreads vastly exceeds the ability to halt or contain them. We can find another especially relevant case in the Boogaloo movement, a far-right anti-government movement in the United States that has used the internet and technologies to promote disinformation, extremism, hate, and authoritarianism, whether on immigration issues, human rights and minorities, feminism, and COVID, attracting new followers to its cause through social media.

3.3. CASE STUDY: CAMBRIDGE ANALYTICA AND THE WHISTLEBLOWERS

For years, the British political consultancy Cambridge Analytica compiled millions of pieces of data from more than 87 million Facebook users without their consent. This information was obtained thanks to the collection and subsequent analysis of thousands of responses and interactions, which allowed them to create psychological profiles of the users. Years later it was discovered that the company used the information for political propaganda and disinformation. This scandal was made public in 2018, after the leak from Christopher Wylie, a former employee of Cambridge Analytica, in separate interviews with The Guardian93 and The New York Times. Subsequent investigations reached the conclusion that the information obtained by Cambridge Analytica aided Donald Trump’s campaign in the 2016 U.S. presidential elections. Likewise, it was considered to have an influence in the public debate in the United Kingdom during Brexit.

This was the goal of Cambridge Analytica. Meanwhile Facebook (Meta) suffered a crisis of reputation that it has still not overcome. The appearances of Mark Zuckerberg94 before the United States Senate and the entire debate that happened during those months in public opinion and among governments and political leaders once again put on the table what role of technology, and its misuse, has on the democratic health of many countries and societies. After the Cambridge Analytica scandal and the macro-investigation in the Mueller report95, which demonstrated that Facebook had been used by Russia to interfere in the 2016 U.S. presidential elections, Facebook has been seen as a perfect tool for spreading content that is not necessarily democratic or respectful and it continues to be in the spotlight of public agencies along with other communications technology companies.

The leak by Christopher Wylie once against highlighted the need to have instruments so that whistleblowers are protected and have channels to make reports, as these individuals are essential for every democratic system. Daniel Ellsberg, William Mark Felt, Edward Snowden, Nicholas Wilson and Sherron Watkins are other well-known whistleblowers, whose cases helped to raise awareness of malpractice and reprehensible and vile acts committed by companies, politicians, and governments in recent decades.

---

94 Senate of the United States of America. Transcript of Mark Zuckerberg’s Senate hearing. 10 April 2018 https://www.judiciary.senate.gov/imo/media/doc/04-10-18%20Zuckerberg%20Testimony.pdf
In 2010 the former soldier and intelligence analyst Chelsea Manning leaked more than 700,000 classified documents to Wikileaks related to the war in Afghanistan and the war in Iraq and exposed cases of violations of human rights and corruption. The United States justice system sentenced her to 35 years in prison, but after seven years in prison President Barack Obama commuted her sentence and she regained her freedom.

The cases of Wylie and Manning were not the first, nor will they be the last. Several debates have opened in all these cases about digital privacy, transparency, accountability, protection and even the concept of national security. All have served to better understand the difficulties faced by whistleblowers who aim to improve the democratic quality of their surroundings, whether businesses, communities, or entire countries, as well as the responsibility of large corporations, including tech companies, to guarantee the democratic health of countries.

Certain governments and institutions have moved to guarantee the protection of whistleblowers in precarious situations. This is the case of the European Union, which in 2019 passed the EU Directive on the protection of whistleblowers. This directive makes it easier to report breaches online and to protect whistleblowers, from employees to former employees and journalists, and it is aimed at making it easier to report irregularities related to EU legislation, as well as, for example, concerning the protection of environmental health, public health, tax fraud, money laundering and offences in public procurement. Sensitive areas over which the European Union has no competency, such as national security, are left out of the scope of this Directive.

---

The competition between different technological models to create and use technology is a central aspect of the bilateral struggle between the United States and China and in the general rebalancing of global power and will continue to be so in upcoming years.

The current geotechnological tension between the United States and China is leading to the creation of two technospheres of influence which are fluid, not sealed off. We come from a bipolar world where the defence of a concrete political, economic, and social model prevailed, which established a certain "balance of power", in which confrontations took place in the peripheral space of their spheres. At present this rivalry is associated with two different models of understanding capitalism or democracy, in which the sides have abandoned balance in search of superiority. Other centres of power, such as India and the European Union, lack strategic advantages or do not have the strength to put another sufficiently seductive model to form a third or fourth technosphere and are hard pressed to find a balance due to the interconnections between all the players, which takes on particular importance in the technological field.

While for decades the international power of the United States was associated with capitalism and the defence of democracy along with certain supposedly universal values, such as the Universal Declaration of Human Rights of 1948, China has clearly identified technological leadership as vital for its current national power, as it holds a fundamental position in the global supply and value chain. China occupies leadership positions\(^\text{97}\) in certain high-tech areas, from the pharmaceutical to the automotive and aerospace industry, semiconductors, AI, 5G networks and robotics.

---

The creation of two technospheres led by these countries along with a growing uncooperative rivalry between them has opened the debate about whether it is even feasible to decouple the technologies promoted by them. If there is no cooperation, one possible solution to keep the spheres of influence free of competitors is to make them airtight. The warnings concerning the risks of a commercial decoupling of supply chains (and critical inputs) and technological and development programmes, to give two examples, show that this would not be easy or viable in the short or medium term.

While the U.S. technosphere model involved a translation of its model of influence and geopolitical networks built since the end of World War II to the digital field, it is interesting to stop and consider the case of China, whose geopolitical network has been growing in recent years after years of ostracism and international self-imposed exclusion. China’s model is being built, in part, through the (Digital) Silk Road, a political proposal from the Chinese government that involves the construction of a global trade network between Asia, Africa, Europe and Latin America that currently includes more than seventy countries. This is a political, economic and trade framework based on incentives to other parties, promoting an enormous array of investments and structural projects, linked to infrastructure and access to strategic raw materials, especially in the global south. This network of alliances and geostrategic interests comes together and converges with traditionally sensitive spaces to the interests of the United States, such as Europe. Italy, the fourth largest European economic power, has joined this alliance, which is strongly opposed by the U.S. and viewed with suspicion by other European countries. This strategy allows China to forge closer ties with many countries and, especially, allows and encourages the participation of Chinese companies in all the projects.

China’s strategy also involves weakening the influence and power of the United States in Asia, as the Chinese government considers the continent its area of influence, creating regional institutional alternatives, such as the Asian Infrastructure Investment Bank and the Regional Comprehensive Economic Partnership, in contrast to other regional and international institutions, such as the Trans-Pacific Partnership Agreement. By doing so, China has managed to weaken the United States’ traditional system of alliances in the region, which, through the Indo-Pacific strategy put forth by the American government is strengthening alliances with governments in the region, especially in the military, cyberspace, and technological fields to counter China’s growing presence. China faces extensive geopolitical tensions throughout the region: from the traditional rivalry with Japan to border tensions with India and maritime disputes with Vietnam, Malaysia, the Philippines, Brunei, and Indonesia.

In the technological sphere, China’s wager and that of its companies is clear: low prices and a digital offer that provides it a competitive advantage over other parties and which has involved several low- and middle-income countries committing to incorporating Chinese 5G, to the detriment of other more expensive options, or having provided access to prized land in the midst of an international dispute over raw materials. While the United States, India and Great Britain prevented the arrival of 5G to their markets, concerned by privacy matters and how it could be used by their customers, South Africa and many other African countries opted for 5G.

The technological war between the two countries has led to greater competition, especially in cutting-edge and vanguard sectors such as artificial intelligence, 5G, and chips and other semiconductors. As competition intensifies, trade and technological decoupling between the United States and China is accelerating.
The dispute between the two nations in the technological field is leading to strong tensions in technological supply chains, an increasingly important tool to achieve geopolitical objectives. The growing technological tension between the United States and China increased, for example, during the Trump Administration\(^\text{100}\), which halted the presence of Chinese technological companies such as Huawei, Tencent, Baidu and Alibaba in the United States, thus harming their global position and restricting and impeding tech transfer to a competitor. Access to rare metals and greater protectionism and nationalist technology policies are a direct consequence of this situation. The United States is taking measures against what it considers an aggressive, unconventional challenge by China\(^\text{101}\).

The events in recent years, from the pandemic to the war in Ukraine, have highlighted the high level of dependency and interdependence between countries in a host of fields: power supply, basic food products, the supply of technological and healthcare components, and elements of security and defence, yet there is also a profound need to increase global cooperation to address shared global challenges such as food insecurity, climate change, the pandemic, and inequalities.

The COVID-19 pandemic offered the opportunity to promote international cooperation between governments, companies, and civil society across the world with the goal of jointly facing the greatest healthcare crisis of the last one hundred years. The outcome of this cooperation has been unequal on all fronts, including the technological front. The scarcity of healthcare material during the first months of the pandemic led to ferocious competition between national governments, and even between regional and local governments, across the world, but also spurred techno-healthcare research to find a vaccine that countered the threat of the disease and encouraged cooperation between the public and private sector. This cooperation transferred to spheres of influence, as was highlighted with the competition for vaccines and other research and development input factors. The application of mobility restriction policies in a large part of the world slowed and interrupted the supply chain\(^\text{102}\) internationally, impacted the nearly all productive sectors, including the tech sector, and caused problems due to a scarcity of products (chips and raw materials, for example) and a widespread increase in prices\(^\text{103}\).

Governments and companies put forward the need for greater strategic self-sufficiency, a fact that has led to a competitive race in promoting national strategic autonomy policies in which technology is one of the main fronts. The European Union, India, the United States, the United Kingdom, Canada, Australia, China, Turkey, Brazil, and a long list of other countries are promoting a race for greater strategic self-sufficiency. The European Union, for example, took a qualitative leap in February 2022 with the approval of the Strategic Compass for Security and Defence after years of joint work\(^\text{104}\). The commitment was clear: invest in “capabilities and innovative technologies, fill strategic gaps and reduce technological and industrial dependencies”. This also includes promoting cyberdiplomacy, establishing a common cyberdefence policy and jointly addressing digital disinformation processes and interference by foreign agents. The Compass offers a long outlook towards 2030 but with imminent tasks, given the international challenges that the EU is facing. The EU is striving to achieve greater cooperation with its traditional partners, such as the United States, Norway, Canada, the United Kingdom, and Japan, as well as other regional partners, such as the OSCE, the African Union, and the ASEAN, and to reorient and promote alliances with Latin American countries.


The pandemic became the great accelerator for digital transformation, with technology at the vanguard of countries’ response to the crisis and with important changes in productive, business, labour, and administrative dynamics. While governments used digital technology to provide an emergency response to a healthcare crisis, companies have taken an important qualitative leap in digital adoption in their supply chains. The start of the war in Ukraine also showed similar shortcomings and needs. The war has once again confirmed many countries’, European countries particular, lack of strategic autonomy in the fields of defence, security, and energy, a circumstance that has been dragging on for years 105.

Another field where this growing rivalry between technological spheres of influence lies in microchips, where both the United States and China are able to project their influence and power through the production chains and exportation. Microchips are one of the clearest examples in which the production chain is regionally fragmented, a circumstance that does not facilitate strategic autonomy, but pushes for greater cooperation between states and between states and companies out of necessity 106. While the world’s main economies—the EU 107, the United States, China, Japan, Taiwan, and South Korea—are promoting their industrial policies to achieve strategic autonomy that attracts the world’s leading chip manufacturers, medium- and small-sized countries that have vast resources in rare metals, essential for chip production, have seen their position in the production chain become stronger. Other relevant geopolitical factors related to microchips are, for example, social stability and the effects of climate change, circumstances that highlight the value of geography.

Microchips have opened a new front in the technological war between China and the United States 108. The decision of the Biden Administration 109 to prohibit access to technology that is essential to China to produce advanced chips 110 led to an escalation of the confrontation between the two governments in the midst of a global semiconductor chip shortage 111 as a result of the increased demand for products that contain chips and the interruptions in the production chain caused by the pandemic. The paradigm in the framework of Chinese-American relations shifted when the national security objectives concerning export controls changed. It went from seeking a relative advantage over its competitors in certain technologies to desiring to “maintain as large of a lead as possible” 112.

Obstructing a rival isn’t enough; investment is essential. Not only is it necessary to prevent China from catching up to the United States technologically speaking, but the technological gap between the two must be maximised. How? Through subsidies. Hence in 2022, Biden launched a large subsidy plan to expand green technology, the Inflation Reduction Act (IRA)\(^{113}\), which includes subsidies and tax breaks valued at nearly 430 billion US dollars, which may harm technological and industrial companies around the world. At the start of 2023 he raised the bar and announced that all construction materials used in federal infrastructure processes must be made in America\(^{114}\): from wood to glass, as well as fibre optic cables. The European Union is one of the first victims of this clash\(^ {115}\), but it is reacting immediately to the American subsidies with the creation of the European Sovereignty Fund\(^ {116}\). These policies show the importance of semiconductors in the technological race, but also of the growing technological conflict between the two powers, which threatens to drag all other countries into a trade and industrial war.

This rivalry has spurred the European Union to engage in intense debates about how to protect its geopolitical space, based on soft power, in an increasingly hostile and interdependent environment. China’s emergence onto the international scene has led the European Union to define itself clearly in recent years. Since 2019, China has been for the Union, first, a “strategic partner”, then a competitor and, lastly, a systemic rival\(^ {117}\). Now increasing numbers of voices are calling to redesign that formula to emphasise Beijing’s competitor role and to move toward the objective of decoupling the EU from the economic and technological dependency of the Asian giant. In the case of China, this means being dependent on components and raw materials. Hence the importance of diversifying. The war in Ukraine and the energy dependency on Russia, especially in the case of Germany and other countries in Eastern Europe, have accelerated the European Union’s plans to reduce its dependency concerning sensitive matters such as energy and technology, committing to self-sufficiency and the diversification of suppliers. Yet the European Union’s plans are not always aligned with the policies of its member states. While the war in Ukraine has highlighted how Germany and other Eastern European countries are dependent on Russia for energy, it is also bringing them closer to China, which is generating a certain level of concern within the European Union.

4.1. The technologies at the centre of commercial (and not so commercial) disputes

Together with the United States and Chinese Governments, companies boast a central role in the current geopolitics of technology. GAFA\(^ {118}\), FAANG\(^ {119}\), FANGAM\(^ {120}\), MATANA\(^ {121}\) and BATX\(^ {122}\). The first four are acronyms that refer to the most important technology companies in the United States, while the last refers to the most important ones in China. All of them lead different statistics in terms of business volume and technological importance around the globe.


\(^{114}\) State of the Union Address. 7 February 2023. [https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/02/07/remarks-by-president-biden-in-state-of-the-union-address-2/]


\(^{118}\) Google (Alphabet), Amazon, Facebook (Meta) and Apple.

\(^{119}\) Facebook (Meta), Amazon, Amazon, Apple, Netflix and Google (Alphabet).

\(^{120}\) Facebook (Meta), Amazon, Netflix, Google (Alphabet) and Microsoft.

\(^{121}\) Microsoft, Apple, Tesla, Alphabet, Nvidia, Amazon.

\(^{122}\) Baidu, Alibaba, Tencent, Xiaomi.
Additionally, they all make up the conglomerate of technology companies that have an increasingly important and decisive role in international dynamics. These tech companies, along with others of lesser importance and international influence, but with added value in the sector, have points in common that should be indicated when explaining their role in today’s geopolitics:

- Their trans-national status. These companies have acquired an international dimension with the ability to influence the practical entirety of the world which goes beyond the country in which they were founded.

- Diversification. These companies are no longer just technology companies. Grow or perish. The follow a single path: mergers and acquisitions. In recent years a notable number of mergers of companies from other sectors (cultural, media, energy, transport, and more) has occurred which has promoted these companies’ role in national, regional, and international dynamics.

- Concentration. Technology companies are becoming larger, limiting competitiveness, and increasing exclusion.

- Their cross-sector status. They have acquired a capacity for influence that goes beyond merely technological influence. They have an increasingly notable capacity for influence in the cultural, social, educational, and healthcare fields.

- The difficulties to regulate them (or control them, in the case of China).

- They are subject to accountability and scrutiny by governments and, increasingly, civil society, not to mention from users and/or clients themselves.

In fact, the role of technologies has also played out differently based on the area where they have grown and built their business. The Chinese model advocates for the primacy of the government, which is the State, while companies are subordinate to it, and civil society is not involved. The United States pools the government’s strength with companies, while civil society plays a subsidiary role in many situations. Lastly, the European Union offers a third model where governments, companies, and civil society have an active, often cooperative, role and where regulation exerts a controlling (and disputed) role. In the United States and Europe, technology companies are a geopolitical representative for nation states.

In the case of China, in recent years the most important technology companies have experienced intervention from the Chinese government, which has led to an extension of its influence over the Chinese technological business sector. This has political, social, and economic implications at the domestic level, but also geopolitical ones at the international level. Chinese tech companies are once again aligning with the Chinese Government and, therefore, the State. When certain Chinese technology business leaders started questioning the Chinese government’s regulatory policies, over the last two years the Chinese government started intervening directly, causing some of these leaders to leave their companies. This is the case of Alibaba’s founder, Jack Ma, who in recent years had criticised the Chinese Government’s regulatory policy and who finally relinquished control of the fintech giant Ant Group, one of Alibaba’s companies. This policy has also involved the Chinese government becoming a shareholder of certain companies. This is the case of Weibo (similar to Twitter) and ByteDance (one of its companies is TikTok).
The latter case is particularly relevant today due to the concerns of many governments from around the world about how TikTok may use the personal data of the users from those countries. This has led to some governments to rethink allowing TikTok to operate in their countries. The United States was one of the first countries to react. In 2020, Donald Trump signed an executive order that prohibited any transaction or business with ByteDance, the Chinese developer of TikTok, which was removed with Biden’s arrival to the presidency, while in 2022 the United States Congress took another step by banning its use on the majority of U.S. Government devices due to matters of national security.

Beyond the specific case of TikTok, the debate about privacy and security is becoming increasingly heated, requiring governments to position themselves or, at least, give warnings to tech companies, in particular foreign firms. In 2020 India took an important step by blocking more than a hundred mobile applications citing questions of sovereignty, defence, security, and public order. Many of these applications were Chinese (among them, TikTok, Alipay, WeChat and Baidu).

One of the most recent cases where the United States - China rivalry has ratcheted up the tension in terms of geotechnology is the rollout of the 5G network\(^\text{123}\), where Europe has become one of the main centres of disputes between the two countries. The Government of the United States, then led by Donald Trump, put the Chinese company Huawei at the centre of this dispute, which the U.S. considered a danger for the country’s national security, and prohibited its use on American soil in July 2020. The U.S. Secretary of State Mike Pompeo left no room for doubts: “The Trump Administration sees Huawei for what it is – an arm of the Chinese Communist Party’s (CCP’s) surveillance state – and we have taken action accordingly.”\(^\text{124}\). A few months before, the Department of Justice had accused Huawei of stealing American technology trade secrets and helping Iran to evade sanctions.

While the Trump Administration clearly sent a signal to one of China’s companies, the British Government under Boris Johnson granted a limited license so that the Chinese company Huawei could build the 5G network in the country. The well-known opposition from Donald Trump’s Administration to the European countries that opted for the Chinese company Huawei in the rollout of 5G became exacerbated. In the end, the British government decided to suspend the agreements with Huawei and ban the purchase of the company’s devices with 5G technology before the end of 2020, as well as to remove every Huawei device before the end of 2027\(^\text{125}\). The United States attracted one of its main partners, the United Kingdom, reeling the U.K. into America’s sphere of technological influence while China kept throwing its fishing hook. In Huawei, the geopolitics of technology had one of its clearest exemplars. In the case of Spain, the country is awaiting the Government’s final decision about which implications the deployment of the 5G network has for national security and how it will affect the partnerships of certain Spanish tech companies with other foreign ones (such as Huawei) based on the recently passed legislation concerning network security and fifth generation electronic communications systems.

Huawei is also at the centre of the technological battle between China and the United States and the construction of the spheres of technological influence in Latin America. The two countries are two of the main business partners for many Latin American countries. In recent years China has launched an offensive to stake its position in the Latin American market. In fact, several Latin American governments have decided to form part of the Silk Road project\(^\text{126}\) promoted by China around the world.

---


The United States, on the other hand, has seen its influence in the region wane significantly. Its foreign policy has been prioritising other regions in the world, such as the Middle East and the Pacific, to the detriment of Latin America. The changing political trends in the region have been questioning America’s interventionist role in the region in recent decades. But technology is another topic, and in this arena all of Latin America has required both China and the United States to boost the area’s growth and development. From necessity comes virtue, forcing the search for balance. Huawei is breaking this neutrality and is requiring many Latin American governments to reconfigure their position, forcing them to decide whether they will allow Huawei to enter in the 5G race or if they will position themselves on the side of the United States.

In the last decade the European Union has done little to slow the increased Russian and Chinese influence in Latin America and the Caribbean, although in recent years it has sent signals that indicate a change in its policies, beyond the objectives of certain specific European countries such as Spain, which has historical interests and ties of cooperation in the region. While the EU published a Global Strategy in 2016, in which it asked countries to promote stronger associations with Latin America, in 2021, this strategy was applied when the EU and Latin America agreed to promote an alliance in the field of digital connectivity, the digital divide and commercial data flows and policies, as well as the regulatory frameworks such as the EU-Latin America and Caribbean Digital Alliance.

The technological sphere of Latin America, immersed in a nebulous cloud, must align and define itself sooner rather than later in the technological field as well, especially when considering the risks and challenges that the region will face in upcoming years.

We can find one further step to understand what role technologies are playing in this Sino-American dispute in the creation of the U.S.-led Clean Network Initiative in 2020, which seeks an alliance of countries and companies committed to democratic values and the implementation of digital trust standards. This initiative has enlisted more than 60 countries and 200 technology companies from around the world, especially in the field of telecommunications. One of the consequences of this initiative was the commitment of the signatories to not work with Huawei on the 5G network.

While the West is creating formal networks of alliances between governments and companies around the world, where democracy and the defence of human and digital rights form part of the letter of introduction, China’s policy cultivates nebulous networks of alliances with nations around the world, regardless of their form of government.

127 Stuenkel, O.; Latin American Governments Are Caught in the Middle of the U.S.-China Tech War. Foreign Policy, 26 February 2021 https://foreignpolicy.com/2021/02/26/latin-america-united-states-china-5g-technology-war/


131 ECLAC. Innovation for development. The key to a transformative recovery in the Latin America and the Caribbean. Santiago de Chile, 2022 https://repositorio.cepal.org/bitstream/handle/11362/47795/1/S2100804_en.pdf

5. THE RULES OF THE GAME OF THE TECHNOLOGICAL REVOLUTION: REGULATIONS

Tackling the challenges of the new digital future requires revising the framework of regulations and competition as it is not possible to face the challenges of the 21st century with the rules of the past. There is a broad consensus that human rights, as we currently conceive them, must also be applied in digital environments. The issue that many governments have been questioning is how, since the current international human rights framework created 80 years ago has logical conceptual gaps due to the technological and digital revolution which did not exist in those years. Even at the level of governance, the difficulties lie in choosing the forum in which to be able to move forward and legislate and establish international standards and regulations. There is no international institution to supervise the few global regulations established on digital matters. While there is an IMF for global payments and a WTO for international trade, the creation of digital governance and a forum for it remains a pending task. Meanwhile, geopolitical rivalries and the incompatibility of governance models are driving technospheres of governance to be created with the risks that arise from them.
The centre of gravity in internet access started in the United States and subsequently in Europe has shifted globally to other economies. Currently, China, India and Indonesia host a third of the global online population. As a result of this movement, the need for global digital governance has encouraged greater competition between the current geopolitical powers, and between democratic and non-democratic governments. The different digital governance frameworks being created nationally reflect the diversity of versions concerning the internet. Here is where the United States, the European Union and China are leading the creation of this digital governance to establish the principles and standards that must govern it. Whoever wins this battle over the rules, standards, and regulations on such sensitive subjects as cybersecurity, data protection and data flows, defence and critical technologies will have a major competitive advantage in upcoming decades.

The governance of technology faces a problem of pace, as the governing and administrative structures of many of these governments are unable to keep up with this rapidly changing digital transformation. This asymmetry involves an evident problem for public policy makers, especially in more complex governmental structures and those which aspire to a common regulatory framework. We should not forget that these power structures were designed 80 years ago, in which the technological race looked very different than it does today. In a globalised technological world, national regulation is insufficient. To overcome these obstacles, there is an urgent need to progress towards a more proactive, comprehensive, and international model of technology governance. The transnational nature of technology poses a challenge for governance that goes beyond national, regional and, even, international administrative limits.

During the G7 summit in 2021 held in the United Kingdom, the participating countries signed a political declaration on digitalisation and technology in which the world’s seven leading economies committed to building “back a better, more productive and resilient global economy, with digital technology at its heart. This should support open societies in the digital and data-driven age, and be guided by our shared democratic values of open and competitive markets, strong safeguards including for human rights and fundamental freedoms, and international cooperation which drives benefits for our citizens, economies and global well-being. We have therefore decided to place the needs of open, democratic societies at the centre of the technology debate and to work together towards a trusted, values-driven digital ecosystem.” The declaration was a clear calling card and, above all, a direct criticism of other models of digital governance based on “government-imposed Internet shutdowns and network restrictions” that undermined democratic values. The G7’s commitment included working together to identify good regulatory practices and to increase cooperation between countries.

For years, the main global political players have been positioning themselves in their commitment to a specific regulatory framework.

China aims to reinvent digital governance and wager on its model of regulation based on cyber sovereignty, in which countries, i.e., governments, exert their sovereignty over information and data. This implies having control of the internet, being able to censor content, accessing online information from the population, restricting people’s access, and promoting technological surveillance on all fronts. At the geopolitical level, China’s commitment to achieve that model is to create alliances with other aligned governments, such as Russia, Saudi Arabia, and Iran, and to try to capture regional and international institutions at the forefront of international regulation.

The European Union is another relevant player in this regulatory battle. It is committed to data protection and thus user privacy, offering a democratic alternative for digital governance. The result is the General Data Protection Regulation (GDPR)\textsuperscript{135}, which has been valid in the EU territory since 2018.

In this race for global digital governance, the United States has shown its concern over the possibility that China may infect other countries with its model of digital governance. One of the latest battles between the different models of global governance was unleashed in the ITU, the UN body that regulates global telecommunications. The recent nomination of the American Doreen Bogdan-Martin as the new Secretary-General of the ITU\textsuperscript{136}, whose commitment to an inclusive digital development model received the support from 172 member states, compared to the 25 countries that supported the Russian Rashid Ismailov, a candidate also supported by China, has been one of the latest frontlines of the digital geopolitical dispute on the diplomatic arena. These elections were seen as a kind of referendum on how the internet should be governed and the two candidacies presented clearly opposed models: one which prized national sovereignty and which prevailed over the human rights and democracy of its own citizens, with the inherent risks concerning governability, and the other that advocated for a free internet that can be jointly governed by governments, civil society, companies and international forums.

Russia and China’s cooperation in the field of digital governance took a qualitative leap in February 2022, a few days before the start of the war in Ukraine, when the two governments published a joint declaration in which they supported internationalising internet governance and committed to a model that took aim at personal freedoms and human rights. The battle for the control of the ITU showed that China and Russia’s support is limited, even in countries from the global south that are highly dependent of the technological infrastructure developed by China and its technological companies.


6. CONCLUSIONS AND UNCERTAINTIES

We are no longer in 1945. The international order that was created then does not fit today's global distribution of power. There is widespread discontent with this status quo, in which new powers are calling for other dynamics of power, cooperation and competition. The geopolitics of technology is not immune to these dynamics. The international structures are still standing due to the lack of viable alternatives.

The pandemic, on the one hand, and the war in Ukraine, on the other, have accelerated the plans of many countries in the search for strategic autonomy in terms of energy, industry, technology, healthcare, security and defence, and more. Both the pandemic and the war revealed national deficiencies faced with a disruptive event on a global scale. This race for autonomy is not without risks, which are associated with the deployment of nationalist, protectionist, competitive and sometimes exclusionary policies. Obviously, we continue to live in a strongly interconnected and interdependent world. The search for allies will be one of the natural outcomes of this situation. This will spur the creation of new strategic alliances between governments, as they seek points of common interests, and strengthen the already existing alliances and update old ones. The spheres of influence between countries, still diluted and fluid today, will lead to greater divergences in the technological field, but for global governance we will need to find these meeting points to address many of the global challenges that humanity currently faces.
The current models of technological and digital governance, led by China, the United States and, to a lesser extent, the European Union, are continually put to the test. There is a need to find representative global spaces for executive discussion and debate. Regionally, the disputes progress and further weaken the ability of these spaces to function. The distances between the leading countries are growing, making it more difficult not only to have international governance, but also to create the spaces for debate. There is the risk that technological advances will go hand in hand with the creation of tech and digital bubbles, with direct consequences for digital rights as a result of technological and digital nationalism. The clash between different regulatory models and frameworks will be inevitable here, not only between autocracies and democracies, but also within these models. Geopolitical tensions also reach the unaligned world, which will see how the major powers compete for their support, or their silence, in exchange for bridging the digital divide. Growing in a world of accelerated (de)construction is extremely complex and represents an enormous challenge.

The current technological environment and, above all, the future will not only change what we do, but also who we are: identity, privacy, consumption, leisure, work, healthcare, personal relations, culture, and much more. The list is vast, limited only by our imagination.

In this technological race, knowledge and geography are at the centre of gravity of geopolitical disputes. On the one hand, the competitive advantage that knowledge offers in the technological value chain has acquired greater weight in recent years, a result of vying for strategic autonomy and disputes between countries. On the other hand, geography and natural resources, following in the wake of knowledge, are universalising the concept of power. Whoever controls the land, whether continental shelves, mining resources, key trading enclaves, critical infrastructures or a favourable climate will have a competitive advantage. Size does not matter. Actors have to be a proactive actor in the technological race.

Within this race from geographical primacy, the geopolitics of fossil fuels still holds a central role in international relations. The war in Ukraine is the greatest example that reflects this reality, as well as the weakness of certain countries, mainly European countries. The rise of renewable energies, an implicit fact in the current energy transition, could well change that status quo. As this energy transition advances, it will decrease the importance of the geopolitics of fossil fuels while during that transition process, fossil-fuel producing countries will have to adapt to the new reality. Adaptation and transformation or irrelevance. The geopolitics of green technology will be even more competitive than the geopolitics of fossil fuels.

In these environments, governments, civil society, and the private sector play an important role, especially in the field of security and defence. Global geopolitical tensions have triggered the deployment of securitising policies across the world, in which technology plays a revolutionary role, impacting in particular the curtailment of rights and freedoms. The different political and social models and projects will be more visible and recognisable in that field. From cybersecurity to technological vigilance. From high-tech military deployment to disinformation campaigns. From election interference to illegal data usage. From the digital divide to the creation of a cultural story. The history of war and international security is the history of technological innovation, and today is no exception. Conflicts will to be increasingly “hybrid” in nature. The speed at which the technological race has taken off means a continual exercise of analysing risks and threats, though also opportunities. In a context of widespread democratic backsliding, power and digital technology must be channelled in the right direction.
UNCERTAINTY 1. FROM STRATEGIC AUTONOMY TO GEOSTRATEGIC CONFLICT

The current technological race has opened several fronts concerning access to resources and the supply of resources and knowledge. Competitive advantage is a vector of influence and power in which geography is central to international dynamics. The pandemic and the war in Ukraine have both accelerated the search for greater strategic autonomy by governments all around the world. China’s dominance in the processing of strategic resources, such as rare-earth elements, key elements in the technological race, and the other powers’ great reliance on these elements generates geopolitical clashes, greater competition and a drive for cooperative projects and processes between allies and partners. Strategic autonomy is not limited exclusively to technology. In parallel, relevant debates about ethics and the environment are (re)opening concerning the access to and processing of resources.

---

UNCERTAINTY 2. DIGITAL DEMOCRACIES versus DIGITAL AUTHORITARIANISM

Technology has blazed an enormous path for governments all around the world to adopt a proactive role in their relationship with their citizens. Currently, democracies are the political system placing greater blame on the (mis)use of technologies, especially due to the impact of both internal and external disinformation and cybersecurity. In turn, on the other extreme we find authoritarian regimes which rely on technology to further control, monitor and interfere in the civilian population, affecting both their human and digital rights.

Governments, civil society, and the private sector have a role to play to protect themselves against the growing threats to cybersecurity and to tackle the controversies that surround technology companies and non-state actors about the illegal use of personal data, surveillance, and electoral interference. The contest for digital global governability between different models will increase geopolitical tensions.

---

UNCERTAINTY 3. TECHNOLOGICAL CONFLICT BETWEEN CHINA AND THE UNITED STATES

The strategic competition between the U.S. and China is spurring global fragmentation in politics and trade, as both countries are focused on promoting self-sufficiency, reducing vulnerabilities, and seeking to decouple their technological sectors. The search for spaces to cooperate on certain shared global problems remains, but the technological and digital fronts and conflicts will remain at risk of further escalation. This conflict will likely drag in other parties who will have to seek a difficult balance given the global interconnections, especially in the technological field.