ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

SCHOOL OF INTERNATINAL STUDIES COMMUNICATION AND CULTURE

DEPARTMENT OF INTERNATIONAL, EUROPEAN AND AREA STUDIES & DEPARTMENT OF COMMUNICATION, MEDIA, AND CULTURE

INTERDISCIPLINARY POSTGRADUATE STUDIES PROGRAMME

«DIGITAL TRANSFORMATION: E-DIPLOMACY, E-CAMPAIGNING AND DIGITAL LAW»

SPECIALISATION: DIGITAL DIPLOMACY

Go with the flow: New frontiers and crossroads for data diplomacy

MASTER'S DISSERTATION

Georgia Anagnostaki

Athens, 2026

Three-member committee

Maria Daniella Marouda, Associate Professor, Panteion University (supervisor)

Vasilis Hatzopoulos, Professor, Panteion University

Andreas Papastamou, Associate Professor, Panteion University

Declaration of Non-Plagiarism and Assumption of Personal Responsibility

I declare that the work submitted as part of my academic studies is the result of my original research. I affirm that it does not make use of the intellectual property of third parties, or any text generated by generative AI applications without proper and necessary referencing. I further confirm that any use of AI in the preparation of this work has been strictly limited to editing and proofreading purposes, without contributing to the creation of substantive content. I acknowledge and assume full legal and administrative responsibility for any instances of plagiarism or academic dishonesty that may arise from this work.

Table of Contents

Table of tables

Table of figures

Abstract

Data diplomacy is an emerging field, responding to the shifting geopolitical and geoeconomic landscape, as driven by the data and AI revolution. This dissertation aims to provide a comprehensive overview of the international relations environment and the effects data have had during the first quarter of the 21st century on diplomacy and foreign policy. The rising volumes and variety of data are rendering them as a strategic resource, mainly due to their economic value, but also for their role in military applications and information weaponisation, all of which contribute to national security. Data are also paralleled to water and oil, due to their strategic importance and economic power. The dissertation explores how these three vital resources intersect and have affected geopolitics, drawing also analogies for the role of data diplomacy today. There are five clustered themes of challenges and risks which data diplomacy faces in the backdrop of contemporary geopolitics. Data governance and infrastructure, security, sovereignty and the datafication of contemporary life are presented and supported by real-world examples. The analysis continues by providing additional cases and synthesising a picture for data diplomacy, organised at global and regional level.

Key words: data diplomacy, weaponised interdependence, data governance, critical infrastructure, sovereignty, datafication

1 Introduction

The internet is a seamless layer of daily life, expanding across all aspects of economic, social, political and personal activities. Most of daily users can hardly visualise or understand it's structure and back-end working-mechanisms, yet rely on it for multiple use cases which have year after year increased the interdependence on internet infrastructure and connectivity[1]. In politics and particularly international relations, this virtual veil has created a kettle of fish all of its own[2]. Thirty-three years after the world wide web went public and the internet looks different, causing societal, economic and political transformations. As artificial intelligence (AI) is now galloping and the hype around it has created immense change in workflows, cultures, circulation of media and information, including the use of internet itself, international relations are faced with multiple dilemmas in byzantine webs of factors and players.

The building blocks of this digital revolution is **data** (Jiang & Martin, 2020). Characterised as the *new oil*, an expression coined by Clive Humby (Arthur, 2013) and later used also by Kai-Fu Lee (Farrell, Newman, & Wallace, 2022), or paralleled with water by a few publications[3], data is considered an asset of power, a borderless strategic resource which provides international players with strategic advantages[4], powering contemporary economies (Szczepański, 2020) like coal and oil did (The Economist, 2017) before the 4th industrial revolution[5]. Data is a driver of social, economic and political transformations,

[1] The latest statistics from 2023 (Ritchie, Mathieu, Roser, & Ortiz-Ospina, 2023) show 67,4% of the global population using the internet. This percentage is an average of global internet users, concealing the disparities between North America and Europe, compared to South Asia and Sub-Saharan Africa, for example. As for the use cases of the internet, these range across communication, learning and education, money transferring and payments, gaming, civic participation, using generative AI, get informed and share news, social interactions (Ritchie, Mathieu, Roser, & Ortiz-Ospina, Internet, 2023 and Eurostat, 2025).

[2] The internet can be considered a predecessor of AI, data-driven and emerging technologies, in terms of the impact it first had on geopolitics and international power dynamics. The levels of connectivity, speed of information sharing, social and political dynamics through social media use, economic transformation and transfer of more power to the private sector (to name a few of the changes it brought) constitute the this "digital revolution" a driver of both innovation and conflict (Chari, 2025).

[3] See chapter 3.2 on water diplomacy for more.

[4] In 2023, free, cross-border data flows contributed $2.8 trillion to the global GDP and it was estimated that this number would reach $11 trillion by 2025 (Basu, 2025).

[5] A transformation driven by trends like the rise of data (McKinsey, 2022).

evident by the weight placed by governments on data governance, critical data infrastructure, cybersecurity and technological sovereignty. All these areas are heavily challenged by supply chain disruptions and trade wars, data flow restrictions and localisation, the dependence on a few owners of software and infrastructure, as well as the growing power of private actors, or facilitated by new partnerships and investments in critical minerals and facilities.

Data diplomacy is a field that first appeared around 2013 to describe data analytics of social media for public diplomacy, only to broaden later to incorporate additional use cases, like data-powered intelligence for better decision making in diplomacy, new topics in international institutions and forums, better services in consular affairs and efficiency in development and humanitarian aid. Despite the terms data, big data and data diplomacy existing for more than a decade, the boom in generative AI changed the playing field in how these terms are studied and referenced. Yet, data diplomacy is viewed narrowly, with the main gaps concerning how data affect the international affairs landscape and diplomacy, by extension. It is therefore significant to not only to take notice of such changes, like observing a natural phenomenon, but to try and extract insights to chart a more strategic path towards lesser interdependence, diversification of sources and protection of strategic interests. History has shown that big technological transformations change the power dynamics globally.

To understand how the latest revolution, being driven by data, influences diplomacy, there needs to be a careful examination of the transformation of geopolitics and international affairs (Chari, 2025).

1.1 Key Concepts and theoretical background

A quarter of this century is past and humanity has already experienced the consequences of massive transformational powers which altered the fundamental structure of society globally. There are several drivers of this change, including the technological transformation of warfare, digital integration and the multipolarity of the world (Osborn, 2025). In a time when economy has ascended as a field of strategic antagonisms and

supply chains are now matters of national security (Platias & Constantopoulos, 2025), weaponised interdependence is a growingly present subject, already discussed by international relations thinkers and publications like Foreign Affairs (Farrell & Newman, 2025) and Policy Journal (Platias & Constantopoulos, 2025). This concept refers to the proliferation of measures of economic coercion, driven by economic interdependence, by states with strong positions on global supply networks aiming to gain more strategic advantages by exercising chokeholds (Platias & Constantopoulos, 2025). As economic security merges with national security (Navarro, 2018), there are certain trends observed amplifying the uncertainties and complex imbalances for governments and the diplomatic corps across the world, like global supply chains, international financial flows, and emerging technological systems (Farrell & Newman, 2025). The increasing multipolarity moves the economic hegemony away from the west and towards "the rest", with the main drivers being India and China. This new economic redistribution also causes geopolitical power shifts, not to mention other external factors, like climate change, migration and naturally occurring resources' reserves, which constitute pressure points to the existing competitions among states (Osborn, 2025). In these power dynamics, the private sector emerged as a player and steadily gains ground and leverage over technological matters (Farrell & Newman, 2025).

In this landscape of geopolitical and geoeconomic conditions, data is deemed as the "lifeblood" of economic development (European Commission, 2020). A 2025 UNCTAD report recognises AI, Big Data, Internet of things and Blockchain as some of the frontier technologies, under the category of Industry 4.0. Frontier technologies are expected to contributed $2.5 trillion in 2023, a number estimated to grow to $16.4 trillion by 2033 (UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, 2025). Each of these technologies are fed by data. For example, AI is the factory processing the raw material (data) into computational products (Zuboff, 2019). Therefore, particularly for the purposes of this paper, behind AI is always massive volumes and varieties of data, the vital resource that powers yet another economic endeavour. All of these technologies are based on data and through a network effect generate even more (Marr, n.d.). The generated data has

grown in the past decade, from 18 zettabytes[6] in 2016 to an estimated of 181 zettabytes in 2025 (Duarte, 2025), while internet users[7] grew by almost 30% in the same timeframe (International Telecommunication Union, Development Sector, 2025). Data needs to be stored, processed and transmitted, which raises the issue of infrastructure, the most important being data centres: material facilities, like warehouses, containing computer servers and hardware tasked with storing, processing and transmitting the data for daily use cases (Alaamer, 2025).

Two terms need to be defined and placed in context here. First, sovereignty is defined as the exercise of utmost political power within a state's own borders (Baylis, Smith, & Owens, 2011), the absolute control of property, resources and individuals for the safeguard of interests and state independence (Dzigal, Safarpour, Godolja, & Susslin, 2025). The other term is national interest, often used by realists to describe what states hold important in pursuit of their survival (Baylis, Smith, & Owens, 2011). This definition not only creates associations with Mearsheimer's offensive realism, but is also linked with the topics of digital sovereignty and a country's ability to safeguard its national interests from foreign interference and "technological coercion" (Ezenwaka, 2025).

Diplomacy is the exercise of foreign policy through peaceful means, like communication and negotiation, by an entity of the international system in order to achieve political goals and objectives (Baylis, Smith, & Owens, 2011). There have been numerous types of diplomacy, relevant to the technological breakthroughs and the 4th industrial revolution, like internet, cyber, tech, digital, virtual, cable and e-diplomacy, each of which slightly differentiates from the next in meaning. These compound nouns refer to the various tools, methods or topics which diplomacy uses or deals with (DiploFoundation, n.d.). Data diplomacy pertains to how diplomacy and data intersect. In order for diplomacy to realise any data-related goals set by foreign policy, it needs to align with other instruments of power, including economic and military (Pavić, Beriša, & Stajković, 2025).

[6] One zettabyte is equal to 1 billion terabytes.

[7] In fact, some regions which demonstrate low internet penetration are estimated to yield even more data in the future (Hinrich Foundation and Visual Capitalist, 2025)

As data becomes an increasingly valuable and strategic resource, its impact on geopolitics and global power dynamics cannot be understated. The control and access to submarine cables transferring data, as well as data centres, can provide certain countries with strategic leverage in the international arena. Furthermore, the complex relationship between diplomats and the Internet industry is evolving, as tech giants often possess more data about a country's citizens than its own government. Understanding all the mannerisms in which data transform the world as we know it, and what will be the role of diplomats in this changing environment, still remains crucial (Jacobson, Höne, & Kurbalija, 2018).

1.2 Research Question

While existing literature examines the visible ways in which data intersects with diplomacy, this paper aims to delve into the less obvious influences of data on diplomacy, **by posing the question of how this valuable resource has altered state priorities, national interests, international cooperation, and national security. It posits that data diplomacy should be understood as a holistic field of foreign policy, encompassing various aspects of international relations related to data, analysing trends, behaviours, and designing strategies towards data-related goals.**

The central research question of this paper focuses on understanding how data, viewed as a resource, impacts foreign policy and international relations, subsequently reshaping diplomacy. This question gives rise to sub-queries exploring the fields and industries impacted by data, the specific challenges faced in foreign policy and diplomacy, the opportunities available to international players through leveraging data, and the connections between foreign policy decisions and the pursuit of data and energy security.

1.3 Methodology

The paper will rely mostly on qualitative methods, analysing news articles and research papers on data centres, infrastructure necessary for data and artificial intelligence, data governance, existing literature on data diplomacy, examples of trade agreements and negotiation hurdles concerning data and their processing etc. The desk research will also

include the analysis of policy papers, AI and data strategy documents, as well as book sources on international relations theory, diplomacy, energy security etc. Graphs and charts were also consulting during this research. Worldwide incidents of infrastructure damages or supply chain interference and their consequences will also be studied, compiled and analysed, as supportive evidence to the research question and sub-queries.

1.4 Dissertation structure

In this first part, the dissertation has introduced the readers to the main problem and research question, outlining major concepts and terms which are relevant to data diplomacy, so as to enhance the comprehension around the matter and hint to more tangible examples. The next part of the dissertation consists of chapters 2 and 3. Chapter 2 aims to outline the existing body of work around data diplomacy and individuate the gaps, which this dissertation aims at contributing. This concerns all the various meanings of data diplomacy, certain gaps that are already understood in literature, as well as other considerations and references to other types of diplomacy around the sphere of data. Chapter 3 endeavours to make a comparative study among data and other resources akin to them, like oil and water, prompted by several analogies detected in the literature between data and oil/water. This comparative study aims to support the position of data as a resource which can and is influencing foreign policy and thus diplomacy, as well highlight the characteristics of this resource.

Having laid down a foundational understanding, the dissertation moves to chapter 4, which discusses notions like data governance, data centres and infrastructure, chip wars, data localization and cross-border data flows, to name a few. For each of the challenges presented, a specific case will be analysed, as an illustrative example of what (and why) transpires. The geographical coverage of these study cases not focus only on the great powers of data, namely the United States of America (US), China and the European Union (EU). There are multiple regional players and smaller powers involved in the data cycle[8],

[8] Extracting, processing, storing, transmitting data and all the infrastructure required for these functions to be effectuated.

that cannot be omitted. The case studies will have the major data powers as poles of interest, around which regional groups and median players will get their spotlight, so long as they have a part in the poles' strategy and data cycle. The dissertation will close with the discussion and brief conclusions, to offer additional thoughts and outline certain limitations, both of this research and of data diplomacy.

2 Literature Review: A deep dive in the hashtag of data diplomacy

Diplomacy, as the "engine room of international relations" (Adesina, 2017), finds itself in a new arena, where variables change rapidly and power and security are not perceived nor acquired as they used to in the beginning of the century. Despite data being discussed for more than two decades now, their intersection with diplomacy and foreign policy seems to have been left out of sight, for the most part. The first mere references in what we discuss today as data diplomacy appear in the early 2010s. Those conversations revolved around the use of data and big data analytics from social media to assess and support public diplomacy, mobile phone data to resolve conflict or remedy natural disasters, knowledge management for organisational and operational efficiency etc. Data diplomacy did not yet exist as a solo term, rather as a concept under e-diplomacy, serving mainly public diplomacy[9]. This trend continued throughout the decade, while data diplomacy was solidified as a term around 2017, when one of the first reports was published from the DiploFoundation, titled "Data Diplomacy: Mapping the Field" (DiploFoundation, 2017), which briefly illustrates the role of data and big data in international affairs and diplomacy. By the end 2020, the literature was enriched by more publications on the subject, although the focus remains the same: how data can support diplomacy as a tool.

Data diplomacy does not have a single definition. It is a cross-disciplinary construct which encompasses a few specific interactions between data and diplomacy, borrowing functions and concepts from science diplomacy and data science, while being heavily

[9] Most of the sources from that time period make reference to public diplomacy and the use of social media and social media data.

linked to digital and public diplomacy. There are three main axes that explain data diplomacy, presented in the following paragraphs.

2.1 Data in diplomacy

Firstly, data is viewed as a tool for diplomacy (data in diplomacy), where data analytics is used to gain insights from large volumes of information, thus adding to the intelligence and knowledge of diplomats and ministries of foreign affairs. This has already had wide and varying applications and it is the first interaction between data and diplomacy that was recognised, recorded and studied since approximately 2012 (Cukier & Mayer-Schonberger, 2013). Influenced by web 2.0 (Marr, 2015), the beginning of user generated content and social media boom of the times, public diplomacy and social media were one of the first applications of data diplomacy, by way of using social media data and analytics to gather insights on public opinion, or information and knowledge about certain situations, specifically in humanitarian aid. For example, using an already existing, free and online mapping platform, Ushahidi[10], volunteers and on the ground responders to the post-earthquake crisis in Haiti in 2010 capitalised on the power of SMS and social media data to develop a "crisis map" (Rocca, Tamagnone, Fekih, Contla, & Rekabsaz, 2023).

If we consider other functions of diplomacy, data can serve as a tool also for information gathering and reporting, providing insights useful for negotiation, as well as for consular affairs. In negotiations, data analytics offer insights to better understanding the various positions and stakes of the negotiating parties, for better development of positions and strategies. Analysis of internal reports and archives of information, as well as organisational structures and operational charts, big data analytics can reveal patterns in diplomatic conduct, offer some predictive capabilities and reveal trends, gaps and needs, whether these can support decision making and strategising, or delivering better services to the public through consular offices. When it concerns public diplomacy and social media, the analysis can concern opinion mining, sentiment analysis and even hashtag tracking, all of which aim at analysing speech trends, public debates and the public's

[10] https://www.ushahidi.com/

opinion on certain topics of interest. Overall, the main diplomatic arenas in which data analytics have a special place: in trade, climate and development, humanitarian affairs, and international law. This is actually quite evident in the humanitarian sector, with projects like GANNET concentrating resources and international actors into a collective effort to build data analytics tools which incorporate AI, with the aim of supporting humanitarians in their work. Big data supplements traditional diplomacy by providing broader insights, corroborating information, and challenging biases, particularly through social media analysis, text mining, and geospatial data. For instance, social media analytics can map public sentiment, while satellite imagery offers objective criteria for negotiations in humanitarian and conflict settings as well as proof of international law violations. In trade, big data improves monitoring of economic flows, and in development, it aids tracking progress toward Sustainable Development Goals (SDGs) and crisis response (Jacobson, Höne, & Kurbalija, 2018).

Challenges of course persist in the area of data analytics for diplomacy. These can be categorised in groups or themes of challenges. To start with, access to data is crucial. As the largest volumes of data are owned by private entities, track I diplomats will have trouble extracting insights from only publicly available data or open sources, like web-scrapping. This matter can be negatively affected by a lesser degree of digitalisation of MFA archives and files, which contain valuable information for data analytics. Another challenge to consider is that of data quality (DiploFoundation, 2017). This issue unfolds several parameters, like the format of data and completeness of dataset, whether access to it was timely and the data was accurate and relevant to the intended objective of use, as well as the complexity of the data. Data accuracy can be further broken down to additional issues, including data veracity and authenticity, which would require data to be accompanied by metadata that would prove these two qualities, to avoid data manipulation. Speaking of, two other challenges that are linked but distinct, are data protection and security. The first aims in ensuring privacy of individuals, communities, vulnerable groups, protection from surveillance and discrimination, while the latter challenge concerns data breaches which occur at an increasing rate. Last but not least is

the matter of data interpretation. While this can be linked to the issue of data quality, this particular challenge concerns the analysis and insights that can be extracted from the data and how one understands them. Misinterpretation can happen if the notions of correlation and causation are not clearly analysed and applied to the data analytics, if there is selection bias towards the data analysed, if there are politicised data in the dataset, or even if the analyst does not have a proper understanding of the context. Similarly, data analysis that has resulted from algorithms can contain biases and misrepresented data, thus need to be a human interpretation to ensure mitigation of this issue. Therefore, while big data offers transformative potential for diplomacy, its integration requires balancing technological opportunities with ethical, legal, and contextual considerations to ensure its responsible and effective use in diplomacy (Jacobson, Höne, & Kurbalija, 2018).

2.2 Diplomacy for Data

Another interaction between diplomacy and data is referred to as “diplomacy for data”, inspired by the “diplomacy for science” definition of the equivalent interaction. This is when diplomacy is the vehicle through which interests on data are promoted, discussed and negotiated, in bilateral or multilateral fora. As Boyd specifically writes, it is “The practice where stakeholders interact to advance data, data use and data interpretation is diplomacy for data”. This is the most straight-forward interaction between data and diplomacy, which other sources (Jacobson, Höne, & Kurbalija, 2018) view and refer to as data being part of the diplomatic agendas. Data as a topic started to be part of diplomatic agendas around 2018, ranging between fields of digital trade, cybersecurity, data protection and international standards.

Certain examples can include:

- the work of the International Data Spaces Association, specifically their endeavours on data standardisation through cooperation and alignment with ISO, IEEE, and the European Standardisation Organisations, to name a few (International Data Spaces Association, n.d.).

- The United Nations World Data Forum which strives to enhance cooperation, increase political and financial capital for data, promote data innovation and secure quality data in favour of sustainable development (United Nations Department of Economic and Social Affairs - Statistics , n.d.).
- The guidelines on global data standardisation developed by the Asia-Pacific Economic Cooperation (APEC, 2020).
- The European Common Data Spaces.
- The Global environmental data strategy, which was recently delivered during the United Nations Environmental Agency seventh session (United Nations Environment Assembly of the United Nations Environment Programme, 2025).

2.3 Data for Diplomacy

Finally, there is a third recognised interaction between data and diplomacy, called *data for diplomacy*. Boyd et al. define this interaction as the "the practice wherein data experts interact to create a platform for relationships is called data for diplomacy", like science for diplomacy, which concerns scientific efforts of bringing nations together to ameliorate relationships. Examples of data for diplomacy can include the UN Global Pulse, which focuses on the best uses of data towards international humanitarian and development work, or the Global Partnership for Sustainable Development Data, a network which uses data to achieve the Sustainable Development Goals (SDGs)[11]. In certain cases, the examples between the various axes of data diplomacy can overlap, particularly between diplomacy for data and data for diplomacy, as the institutions and bodies carry a wide range of responsibilities. The UN World Data Forum is a *diplomacy for data* initiative, as it constitutes a core space for discussions that advance data and innovation, led by the UN itself, a primarily diplomatic body. It also resulted into a written document, satisfying the parameter of "data on the diplomatic agendas", namely the Cape Town Global Action Plan for Sustainable Development Data[12]. Simultaneously, the Forum can be considered as a *data for diplomacy* example, as it involves a variety of stakeholders whose work interacts

[11] https://www.data4sdgs.org/
[12] https://unstats.un.org/sdgs/hlg/Cape-Town-Global-Action-Plan/

with data, using the forum as a platform to advance relationships around their interests, thus advancing diplomacy.

These three axes of data diplomacy (data in diplomacy, diplomacy for data and data for diplomacy) cover most of how data diplomacy is understood, especially in relation to science diplomacy. Other than Boyd et al., sources converge on the first two axes about data in diplomacy, where data is seen as a tool that enhances diplomatic functions, and diplomacy for data, where data becomes a topic for discussion and negotiation. Data for diplomacy has only been found to be referenced in the work of Boyd et al, particularly with the specific definition given.

2.4 Other aspects of data diplomacy and literature gaps

Is there a fourth manner in which data and diplomacy interact? Jacobson, Hone and Kurbalija in their 2018 report for DiploFoundation do not mention *data for diplomacy* as the third branch of data diplomacy, rather focus on the impact data can have on "the environment in which diplomacy operates", meaning any shifts in international relations, geopolitics and geo-economics that can be attributed to data as a factor. This fits better the pattern that regularly appears when studying the internet and the digital sphere and its interaction with diplomacy: exploring how it changes the environment of international relations and foreign politics, identifying how it has become a topic of diplomatic agendas, and then viewed as a tool that enhances efficiency, which is typically the field drawing most of the focus. Similar to the study of data's influence to diplomacy, studies had previously focused on the Internet's effect on it. Internet used to be (and still can be) a tool to make diplomacy more effective, efficient, and inclusive, captured in the concept of e-diplomacy. It also brings new topics to diplomatic agendas, whether it relates to international negotiations on cybersecurity, the promotion of multilingualism online, the establishment of a global Internet infrastructure, or the discussion of cross-border e-commerce rules; all of this is captured by the term *internet governance*. Similarly to data, the Internet has affected the environment in which diplomacy is practiced, causing shifts in geopolitics and geo-economics, from the physical position of the main Internet cables

that carry data and the data centres that host data, to the consideration of data as a national asset, not unlike the importance of oil for the traditional economy.

Data in diplomacy is more widely documented and analysed, both in academia and in several web posts of think tanks and institutions. When data diplomacy is used as a compound noun, it mainly refers to the benefits of using (big) data analytics in diplomatic corps, for better insights and intelligence in the core diplomatic functions. Though it is the axis most researched and reported on, there are still gaps in the literature, like studying specific cases of data usage by Ministries of Foreign affairs (Jacobson, Höne, & Kurbalija, 2018), or gaining insights and testing the interaction of AI with data diplomacy. Still, the other aspects of data diplomacy (agenda topic, environmental changes, data community cooperation etc) seem to lack adequate representation in the existing literature as it is.

Still lacking any space in academia and research, the literature on data and their influence on international relations and diplomacy is quite fragmented, and mainly occurs in news reporting and articles in foreign affairs new outlets. Such sources refer to the trade rivalries between states, how supply chain risks threaten the computing power and security of infrastructure, how data governance is posing challenges of its own that appear in the form of data localisation and cross-border data-flows restrictions etc. It seems that data diplomacy, governance, sovereignty and other connected concepts have been studied mainly through the lens of private entities and individuals. Even data diplomacy, which should strike as a topic studied under the scope of international relations, is referenced in publications in the context of private companies or individuals and the diplomacy that happens among them concerning the handling of data (Boyd, Gatewood, Thorson, & D. V. Dye, 2019).

There is still quite a lot to be explored around data diplomacy, even as this chapter has already mentioned several gaps in the field. The research community needs to study and highlight all the shapes and forms in which data affect diplomacy, to “inform diplomatic interactions” (Boyd, Gatewood, Thorson, & D. V. Dye, 2019). Data diplomacy is not attributed the significance and weight it requires. It should be a distinct field of study and

of diplomatic practice, away from other types of diplomacy related to digital technologies. The literature showcases that data diplomacy is mainly understood through the scope of data analytics, with benefits tied to public diplomacy and social media analytics; these uses and interpretations of data diplomacy are not the only ones, as already analysed in this chapter, but they are the most prominent ones in the literature. This is a shortcoming, not only of the academia, but also of the diplomatic community as well. Not only because the diplomatic corps shall continue to be unequipped for the data challenges that arise, but also because there seems to be a narrow understanding of the extent and the significance of data and its influence to diplomacy (Boyd, Gatewood, Thorson, & D. V. Dye, 2019).

3 Drawing the parallels: resources that influence geopolitics and diplomacy

There have been numerous nouns and adjectives added next to *diplomacy* to specify a context, give specific meaning or denote a specific objective of the diplomatic practice. Peripheral diplomacy, science, environmental, climate, water, oil, digital, public, maritime, cultural diplomacy, sport diplomacy, health and energy diplomacy, citizen diplomacy, to name a few (College Hive, n.d.). As diplomacy has grown over the course of human history to include functions and fields beyond inter-state negotiations, it is important to recognise its various types, before drawing any parallels. These types reflect how human creativity influences the practice of diplomacy, incorporating new means and tools that upgrade and facilitate the conduct of diplomats, while the field has become inclusive of non-state actors/representatives and more nuances between the areas and topics of foreign relations (Kurbalija, 2025). The various types of diplomacy can be categorised in three distinct contexts: geopolitics and geo-economics, topics addressed by diplomacy and methods or tools for conducting it. For example, AI, chip and oil diplomacy fall under the geopolitics context, semiconductor diplomacy under the topics addressed and bilateral, public or metaverse (also known as virtual) diplomacy are types of diplomacy that refer to the methods and tools used for the practice. These examples were based on the table shared by DiploFoundation on their website, which contains 136 uses of the term

"diplomacy" under each of the aforementioned categories. A copy of the table with diplomacy types relevant to this paper is presented below:

Table 1: Types of diplomacy per context of use, selection from source: DiploFoundation. (n.d.). Types of Diplomacy. Retrieved from diplomacy.edu: https://www.diplomacy.edu/topics/types-of-diplomacy/

Types of diplomacy[13]	Diplomacy and Geopolitics	Diplomatic topics	Diplomatic methods and tools
AI diplomacy	Yes	Yes	Yes
Blockchain diplomacy		Yes	
Cable diplomacy		Yes	Yes
Chip diplomacy	Yes	Yes	Yes
Cyber diplomacy		Yes	
Data diplomacy		Yes	Yes
Digital diplomacy	Yes	Yes	Yes
Hybrid diplomacy			Yes
ICT diplomacy		Yes	
Internet diplomacy			Yes
Metaverse diplomacy			Yes
Oil diplomacy	Yes		
Online diplomacy		Yes	Yes
Quantum diplomacy		Yes	Yes
Raw material diplomacy		Yes	
Science diplomacy	Yes	Yes	Yes
Semiconductor diplomacy		Yes	

[13] Energy diplomacy was not included in the table of the source website.

Tech diplomacy	Yes	Yes	Yes
Virtual diplomacy			Yes
Water diplomacy		Yes	
Web diplomacy			Yes

The main focus of this chapter is to draw a parallel between water, oil and data, as three distinct resources with ties to diplomacy and heavy influence on geopolitics and international relations. Water and oil are selected specifically for their relation to data and the similarities drawn by several authors and publications (The Economist, 2017 and Deakins, 2017). However, the recent hype with AI has highlighted that water and oil (or energy in general) are affected by data themselves; more particularly, by the need for data and the demand to process it. Therefore, data, water and oil are interconnected because they affect each other, or simply because data is adding a stressor on both oil (energy) and water policies.

3.1 Oil Diplomacy

The comparison between data and oil was drawn back in 2013 by an article in the Guardian and later on reiterated by the Economist on 2017. The phrase “data is the new oil” is attributed to Clive Humby, a Sheffield mathematician, who is said to have said it twenty years ago (Arthur, 2013). Although Humby was mostly referring to the monetary value which data brings to industries, like oil was (and still is) doing before big data became a lucrative commodity, the similarities with oil reach much further. Like oil, data is more valuable after it has been processed and refined, which by extension means that the players in this field, like Amazon and Google, profit best when they possess the ability to store and transform data into insights or products. Data has increased tenfold in the past decade, driven by web 2.0 back in 2005 and continued with each social media application or internet usage that emerged (Marr, 2015).

Basically, the internet is consisted of data (Jiang & Martin, 2020), while internet usage produces more of it[14] (Marr, n.d.). Simple daily activities for which people use the internet, like Google search engines, tracking exercise with a smartwatch, scroll through social media or look for products to buy on online marketplaces like Amazon, leave a digital trace of data that inform the companies like Facebook, Amazon, Google (Alphabet) and Microsoft. This raises the concern of control over data. These companies are like "data distilleries", using this raw material to profit directly off of it by improving their products or their advertising space, or sell data-driven information to other entities (The Economist, 2017). This is where oil and data converge: both are resources which have massively fuelled economic activities and industrial revolutions. Data centres mean now what oil refineries meant sixty years ago, only with different functions (The Economist, 2017). Oil propelled the mass production of physical items and greatly covered the energy demands of over-consumerism in the past years, while data fuel the digital economy. Today, oil and energy are still used as a geopolitical tool in the pursuit of national interests (Ahmed, 2025). However, as seen in chapter 2 as well as in the categorisation of the various diplomacy types in Table 1, data diplomacy is still not referenced in the context of geopolitics. Lastly, there are new legal mechanisms to exert power and control over data, like the GDPR (2018) or the USMCA/CUSMA (2020)[15], so did international law for fossil fuels and natural resources (Schrijver, 2008).

The similarities between oil and data might stop there. Oil is considered to be a finite resource. On the other hand, data is produced by a network effect of connectivity; the more users and consumers are active online, the more data is being produced, a trend enhanced by the internet of things and the web of people and devices online[16]. It's like people are miners, living in the mine. Data's value grow's exponentially, with every processing, analysing and sharing of it (Ashton & Forder, 2024). Also, data is a reusable

[14] Or, as the saying goes: if you're not paying for it, you are the product (Goodson, 2012)
[15] This was a first major trade agreement putting in place data flow and digital trade provisions.
[16] "For example, data is both created and used by autonomous vehicles interacting with connected infrastructure in a smart city." (Schlosser, 2018)

resource, which keeps and eve augments its value with every further use, while oil is a single-use resource and has value per unit sold and consumed (Schlosser, 2018).

It is important here to go beyond the comparison of the two resources and discuss the term of oil diplomacy, in order to compare with data diplomacy terminology, context and application of the term in academia and practice. In academic literature, finding an exact definition for oil diplomacy is challenging. Oil diplomacy is a subset of energy diplomacy, and refers to using diplomatic means to achieve political or economic objectives concerning oil, relevant mainly for oil-importing countries (Hartshorn, 1973), or using oil to achieve other political and diplomatic objectives, which is often practiced by oil producing and exporting countries (DiploFoundation, n.d.). Particularly in the 20th century, post-World-War-II era, when the oil reserves that started being operational in the Middle East and other oil-rich regions had heavy impact on the energy scene (DiploFoundation, n.d.), the importance of oil diplomacy became quite evident around oil crises, like the 1973 OPEC embargo (Ahmed, 2025). On the other hand, data diplomacy is mainly referenced in the context of diplomatic tools and methods, or topics, and much less in the context of diplomacy and geopolitics. Data is rarely considered a driver of foreign policy and diplomacy, in the way oil does, notwithstanding being repeatedly valued as the “new oil” or the “most important resource”. This is a gap that must be addressed, not only in academia, but in the diplomatic conduct and general study of international affairs.

3.2 Water diplomacy

There is a contradicting rhetoric, which instead of comparing data to oil, compares it to water. The main reason for this alternative narrative, as detected more often in articles which comment on the topic, is the matter of data affluence. Water is a more abundant resource compared to oil and so is data, which is also growing in volume by any digital trace left online (Deakins, 2017). Other arguments highlight the importance of data cleaning and data quality (Ambler, n.d.). In fact, data can pose as a severe issue when unclean and erroneous, causing glitches in the software and algorithms and undermining

entire servers and services. Such an example is the halt of trading of Nasdaq, back in 2013 (Arthur, 2013).

There are also certain lexical similarities used in both water and data related descriptions. Water is a transboundary resource which holds various meanings across the stakeholders and contexts involved. It can be a cultural, political or economic good. A similarity shared by oil and water is that geography deals a good hand to some countries compared to others. With oil, it is mainly countries which hold oil reserves that have a strategic advantage over it, while with water, the upstream country is the one favoured by geography. In both cases, manipulating the "flow" of the resource is crucial for maintaining a bargaining chip and exerting power over other states, whether these are downstream states, or importers of these valuable resources. While oil is not transboundary, data definitely is. The internet is borderless, a trait shared by its building blocks (data), which explains the race for asserting sovereignty of data, by creating governance regimes and trying to influence other states to adopt them[17] (Jiang & Martin, 2020). The cross-border nature of certain river basins, in conjunction with the various meanings that water holds (economic, political, cultural) create a bigger surface area for distinct interests between stakeholders and therefore conflicts (Vij, Warner, & Barua, 2020).

According to Dan Vesset, Group Vice President, Analytics and Information Management at IDC, compared data to water in saying that "data needs to be accessible, it needs to be clean and it is needed to survive" (NODE, 2020). By making such a statement about the vitality of data, Vesset elevates data to a new type of resource, one that is not only significant for economic activity, innovation or growth, but a resource on which survival is depends. In this light, when considering that the quality and accessible quantity of water is also another matter that affects political relations and conflicts across regions which

[17] As further analysed in Chapter 4.3, data governance regimes have heavy geopolitical consequences and objectives, as a data governance scheme influences the digital economy, digital and data trade, as well as disrupts the activities of private companies (Jiang & Martin, 2020). Therefore, countries which still have not developed their own data laws, are influenced by the existing relationships they have with allies, depending on which geopolitical sphere's influence they are under.

share water sources (Vij, Warner, & Barua, 2020), can't the same assumption be made about data in the future, or yet the present?

The reasons why water and data can constitute matters of security might become clearer when recalling the meaning of 'old security' and 'new security'. Old security was all about securing geographical borders, mostly with military means, as it came to be for Westphalian states, according to Mackinder (Mackinder, 1904). New security, on the other hand, takes into consideration types of security at both personal and national levels, as defined by the United Nations Development Programme (1997), ranging from economic, environmental, personal, community, political etc. While water or data might not be explicitly mentioned as categories here, they are both elements whose security and access have been elevated as fundamental to the new security considerations.

As for a definition for water diplomacy, it places water as an issue in the foreign policy agendas, with long-term objectives beyond water crisis management and conflict prevention. Water diplomacy objectives range from improving regional security and stability, promoting regional integration, boosting trade relations, to increasing political influence (Zhang & Li, 2020) (DiploFoundation, n.d.). The politics around water geographies, power asymmetries and conflicts over this resource are mostly overlooked, while international law is yet to be proven a successful mediator over transboundary water issues (Vij, Warner, & Barua, 2020). The way water diplomacy is treated, based on Vij, Warner and Barua (2020), can be assimilated to the gaps detected earlier, in the literature review for data diplomacy. While oil diplomacy is placed in the context of foreign policy, geopolitics and international relations, being considered as a factor of shifting power dynamics and a means of fulfilling diplomatic objectives, scholarship does not treat water and data in a similar manner. This is particularly odd, considering the value placed on data, as discussed so far.

3.3 The impact of data on water and oil

The three resources (water, oil, data) do not only intersect with similarities and differences between them, in how they have been influencing geopolitics or how they have been

utilised civilisation. There is also a one-way relationship, with data on the one end and water/oil[18] on the other, in which data and its ever-expanding dominance in technology and economy have a huge effect on energy and hydro resources. Data centre infrastructure alone, which supports cloud and AI functions, bares huge environmental costs, due to their rising demands in energy and water, for powering the data centre and cooling the servers (Spindler, Fisher, & Atamian Hahn-Petersen, 2025). Based on a report by the Hinrich Foundation and Visual Capitalist (2025), in 2022 data centres consumed 292 million gallons of water and 460 terawatt-hour of electricity. These numbers are projected to grow to 450 million gallons of water and 800 terawatt-hour of electricity by 2030 and 2026 respectively, based on the same report[19]. Data centres also have indirect energy and water needs, driven by the demands in extraction of critical minerals necessary for hardware (Hodgson, 2025).

The issue has already been addressed by the United Nations Environmental Programme (UNEP), which released a set of procurement guidelines for authorities and organisations to reduce the energy and water demands of data infrastructure (United Nations Environmental Programme, 2025). Apart from infrastructure, generative AI and large language models (LLMs)[20] form the inference stage, which has become equally demanding as the training phase, while there are other direct impacts to consider, like the energy consumption to mine the mineral resources for the hardware, or even the e-waste and emission produced from running the software (United Nations Environment Programme, 2024). These demands in energy and water have greater impacts in the areas

[18] Oil is one of the biggest energy resources and has had a great impact in geopolitics, as illustrated in chapter 3.1. In this chapter, it will be used interchangeable with the words “energy” or “energy resources”, since there is an already established relationship between data and oil in the text, but data impact the energy sector as a whole.

[19] Estimations will vary across different sources. For example, there are estimates that by 2027, AI adoption could cost 4.2 to 6.6 billion cubic metres (or 1.11 to 1.22 trillion gallons) of water withdrawal by 2027, for both onsite cooling and offsite electricity generation purposes. (Spindler, Fisher, & Atamian Hahn-Petersen, 2025).

[20] “Large language models (LLMs) are a category of deep learning models trained on immense amounts of data, making them capable of understanding and generating natural language and other types of content to perform a wide range of tasks […] LLMs represent a major leap in how humans interact with technology because they are the first AI system that can handle unstructured human language at scale, allowing for natural communication with machines.” (Stryker, n.d.)

surrounding data centres (usually residential, even though rural), stressing the electricity networks and water provision to residents (Fleury & Jimenez, 2025). Longterm, these impacts are likely to affect decisions concerning the location of data centre development.

3.4 Other analogies

Before proceeding to the next chapters, it is valuable to draw a few more analogies regarding data. During this research, two online publications were found to link data with uranium yellowcake[21]. Data grows in scale and variety, becoming potentially unmanageable. The volume alone will create not only storage problems but also data protection and security problems, a metaphorical "data Chernobyl" (Pesce, 2024). Similar to yellowcake, data also needs careful handling during processing and refinement to yield insights; this care is not only limited to proper pre-processing, like mitigating bias and cleaning, but also ensuring data protection and preserving security from breaches (Ashton & Forder, 2024). Therefore, the entire analogy rests on the point of data security and the immense (potentially catastrophic) impacts this might have for organisations responsible for data security[22].

On another note, data is not inherently as damaging as oil or uranium. Instead of focusing on data's qualities like being a driver of the economy, or needing extraction, storage and refinement to yield value, this new analogy provides a more positive outlook: data is like soil. The analogy with soil makes one think about qualities like cultivation, care and attention. Soil is an ever-changing ecosystem which contains valuable nutrients, while needing work and cultivation to yield "crops", while innovative techniques will yield more for less. There are also different types of soil, similar to the different types and contents of datasets and databases, each requiring their very own treatment, based on proper contextual understanding, to provide the correct insights. Lastly, soil, data and water share the need for quality (Inteliment, 2024).

[21] Concentrated form of uranium oxide, containing 70-90% of the element (Taylor & Francis, n.d.)
[22] More on data security is analysed in chapter 4.2 "Security: cyberspace and critical infrastructures"

The respective compound nouns for diplomacy concerning uranium and soil are nuclear diplomacy and earth or environmental diplomacy. Both are treating the first noun of the compound as a topic on the diplomatic agenda and do not earn a position neither in tools nor in geopolitical contexts (DiploFoundation, n.d.).

4 Challenges on the intersection of data and international relations

The data revolution (European Commission, 2020 and Wriston, 1997) has produced a series of chain reactions for all the major players of the field, state and private alike. Reactions as such include the designation of a Commissioner for Tech Sovereignty, Security and Democracy, a portfolio aiming to highlight the importance placed by the EU on digital diplomacy, frontier technologies and data in the context of security and democracy[23] (Ricart, 2025). Reactions can also come in the form of new priorities, partnerships or "divorces" in the international arena (Chari, 2025). So, what drives these manoeuvres?

The European Strategy for Data identifies several problems to overcome in order to achieve its vision: data availability, imbalances in market power, data interoperability and quality, data governance, data infrastructures and technologies, skills and data literacy and finally cybersecurity. These reflect several patterns noticed in the public discourse and scholarship concerning data[24] of drivers or inhibitors of data-related policies and actions, related to overarching issues like sovereignty, infrastructure, governance and security and their effects on exercising foreign policy.

It is noteworthy that the EU stance altered in the second Von der Leyen mandate after 2024, focusing more on economic security, a development tied with retreating from regulation and focusing on industrial policy and competitiveness (Ricart, 2025). Meanwhile, the alternating retaliations between US and China have intensified during

[23] It is very interesting how this role combines technology, security and democracy, as a triangle which can only stand if all three sides are present simultaneously, working as conditions for prosperity.
[24] Namely news articles, commentary from international institutions, academic papers, policy documents etc., which have been researched and studied for this dissertation.

2025, while the rest of the players keep working towards achieving their data strategic goals[25].

This chapter identifies certain axes of risks and challenges faced by international state actors concerning data and narrates how these intricate relations between them are reformulating accordingly.

4.1 The gold rush of critical data infrastructure

As it happens with "mining" activities for fossils and mineral resources, from gold to oil, equipment and technological know-how is required to tap into the potential of data[26], too. The metaphor of a data gold rush, as cliché as it sounds (Peters, 2012), is resurfacing, highlighting the significance of data infrastructure for "mining" this valuable resource (Rossi, 2015). Data centres are like oil refineries: infrastructure which ensures the vital resource that is mined gets processed to allow companies to extract value[27] (Krantz & Jonker, 2025). Especially after the AI upsurge, computational power has been pivotal for the prosperity of the sector. This means that private companies which rule the infrastructure and hardware sector, like NVIDIA[28] and Oracle, but also energy providers[29], are increasing their gains, especially considering the oligopoly of the sector (Taylor J. , 2024). In fact, AI infrastructure investments range in the billions, with US companies pledging $500 billion in the next four years, and Europe announcing €50 billion, while France another €109 billion internally (Bou, 2025).

This investment rush will not only affect private companies on the receiving end of the investment. World over, governments have high stakes on the data centre bet, as these

[25] For instance, Brazil and Chile are attracting investments for data centre construction, due to their high capacity in renewable energy (Gandhi & Chandran, 2025).
[26] "The 1800s were all about mining – gold, iron and other metals. The 1900s were all about drilling – oil, natural gas and shale oil. The 2000s are again going to be focused on mining, but of a different kind – data." (Rossi, 2015)
[27] The value of data is information and insights, or data-driven products, like new software and machine learning models, AI-powered assistants and chatbots or generative pre-trained transformers (see ChatGPT, LeChat or GANNET).
[28] NVIDIA went from an evaluation of $1 trillion to $4 trillion in just two years, reaching this milestone earlier in 2025 (Mickle, 2025).
[29] Energy demands are projected to reach between 122 to 219 gigawatts by 2030 (Bou, 2025).

facilities constitute critical infrastructure. These assets are proving to be the backbone of modern connectivity, powering everything from cloud services to AI (Spindler, Fisher, & Atamian Hahn-Petersen, 2025). The data centre industry's worth is projected to be more than $584 billion by 2032, while estimated to be handling over 95% of internet traffic globally. As with any critical facility that affects interconnected interests, data infrastructure is a bone of geopolitical contention (Alaamer, 2025), touching upon data centres, subsea cables, satellites, semiconductors and chips, supercomputing elements, energy and critical resources necessary for their constructions and maintenance (Alaamer, 2025). This hardware necessitates a variety of minerals and metals, such as gallium, germanium, metallic silicon, tantalum, platinum-group metals, copper[30], rare earth elements, silver, and gold (Stacciarini & Gonçalves, 2025). Correspondingly, the energy needs of these facilities are rising[31], causing the clean and renewable energy sector to boom, as states struggle to find the appropriate energy sources to cover their data-demands (Ahmed, 2025). Consequently, the energy needs are another factor driving the demand for critical minerals and rare earths, adding another stressor in the data diplomacy agenda.

Although the amount of minerals required for data centres has not been concretely identified, geopolitical rivalry is already causing supply chain disruptions, perceived as threats to the sector's security and growth (Stacciarini & Gonçalves, 2025). This is part of the weaponised interdependence and supply chain chokeholds as a means of coercion. Case in point is the US-China back and forth rivalry of export restrictions. China has risen as a sizable rival against the US technological dominance of the previous years (Allison, Klyman, Barbesino, & Yen, 2021), with TikTok challenging Meta's dominance and Huawei rising as a competitor in network infrastructure (Lehdonvirta, Wú, & Hawkins, 2025). Specifically on data and AI, each country has an advantage, with the US dominating AI-products' manufacturing, while China holds critical minerals necessary for the sector's

[30] The demand for copper is in fact so high, for digital and clean energy infrastructure, that new hubs of extraction are spurring, like Chile. The need for copper in data centres is estimated to increase six times over by 2025, while already creating deficits in supply by 304.000 tonnes in 2025 alone (Hodgson, 2025).
[31] See chapter 3.3 "The impact of data on water and oil

infrastructure, like gallium, germanium and rare earths[32]. In 2022, the US imposed restrictions on exports of advanced AI chips and semiconductor manufacturing equipment. In 2023, China responded with gallium, germanium and rare earth export limits, while the US hardened AI restrictions, specifically requiring that NVIDIA to stop exports of previously compliant AI chip models. The administration involved also the Taiwan Semiconductor Manufacturing Company (TSMC), requesting similar measures[33]. Even though the two states recently came to an agreement about NVIDIA H200 AI chip export from US to China, which Trump allowed at the condition that the US government would get 25% of the sales revenue (Breuninger, 2025), China halted the import. This move has been criticised, as internal semiconductor production is insufficient for the growing needs of the Chinese AI sector (Kasanmascheff, 2026). This highlights the persisting interdependence of the two.

The game between US and Europe is different. With 4,165 facilities, it is undoubtable that the US is host to the lion's share of data centres, followed by Europe with 3,476 (Lu, 2025). Although there are no clear statistics on the ownership of the European data centre infrastructure, PIMCO, a US asset management company, was recently awarded a significant contract European Data Centre Fund (D'Souza, 2025), while American tech giants have infiltrated the continent with several projects of data centres and cloud infrastructure. This contrasts the recommendations of policy officials on how the EU should promote digital sovereignty to safeguard resilience (Ricart, 2025), particularly in the climate of foreign stressors and coercion by the current US administration. The location of data infrastructure raises the stakes also for data governance and data sovereignty, reducing state control over personal and non-personal data, delaying access of authorities to national data when stored abroad and relinquishing the opportunities for taking advantage of domestically produced data for research and innovation (see chapter

[32] China holds 90% and 60% of gallium and germanium global production respectively (Stacciarini & Gonçalves, 2025). However, China's power in this sector comes mostly from its control over economic and technological means of extraction and processing power (Farrell & Newman, 2025).
[33] NVIDIA and TSMC dominate the semiconductor and AI chip market (Stacciarini & Gonçalves, 2025).

4.3 and 4.4). This can also be taken as an analogy between US and China and other countries dependent on them for infrastructure access.

Geography also comes as a factor to data infrastructure. Countries which hold disputed waters or have strategic maritime positions can manipulate cross-border routes of sub-sea cables[34] (Hinrich Foundation and Visual Capitalist, 2025). The states around the Red Sea and the Persian Gulf are particularly well situated in this regard, holding the passage of 90% Europe-Asian data traffic through subsea fibre optic cables, thus having leverage to position themselves differently on the global scene and ameliorate their influence in elevating the global south into this AI revolution (Cohen, 2024). Other factors in excellent geographic positions for data infrastructure are land availability and cool climates. Data centres need sizable areas, ideally well connected to electricity grid and situated in colder climates, due to the square meters required to host all the hardware for computational power and high electricity demands. The heat emitted by data facilities creates the necessity for cooling equipment, the costs of which rise in hot climate, ultimately raising energy needs and overall operational and maintenance costs[35], decreasing efficiency (Gandhi & Chandran, 2025 and Einhorn & King, 2025).

Such geographic factors pose an opportunity for diplomacy, in creating the right partnerships and cultivate relations that will allow states to cooperate on resolving such challenges. Europe is well positioned, considering the technological innovation level of Nordic countries, combined with the cool climate of the region and the well-developed green energy grid. Capitalising on these conditions can lead to a regional data hub creation for hyperscalers (Cohen, 2024), essentially boosting innovation and entrepreneurship and reducing foreign dependence and coercion. In the contemporary political context,

[34] Subsea data cables transmit data and power across vast distances and continents, but widening their instalment is met with geopolitical and environmental resistance (Hinrich Foundation and Visual Capitalist, 2025).

[35] Also, due to heat inflicting physical damage which creates repair costs and losses from operational interruptions (Einhorn & King, 2025).

domestically controlled data infrastructure is as crucial as controlling energy resources (Esposito, 2025). Is it achievable?

4.2 Security: cyberspace and critical infrastructures

There are two types of attacks relevant to data which concern governments: attacking critical data infrastructure, like submarine cables and data centres, or cyber-attacks which cause data breaches or obstruct the functionality of general critical infrastructure. Information infrastructure faces increased vulnerabilities towards attacks, with consequences of unprecedented magnitude (Wriston, 1997). Attacks on such facilities are not even able to be classified as acts of war, as usually the enemy cannot be identified and the damage of the attack might not be determined to qualify as such. As these cyberattacks become more sophisticated and frequent, the costs will be higher, especially against AI-powered attacks, which can bypass existing capabilities to counter them. Simultaneously, cyberattacks against critical infrastructure have transformed into coordinated efforts, perpetrated both by state and non-state actors. (Singh, 2025)

Apart from cyberattacks against critical infrastructure, there are examples of real-world destructions, specifically of undersea cables. In November 2024, two cables were severed in the Baltic Sea, a suspected attack from Russia (Hinrich Foundation and Visual Capitalist, 2025). Russian was involved in damaging the Estlink-2 undersea cable in the Gulf of Finland by dragging an anchor over it, while the Chinese vessel is suspected of having deliberately cutting the C-Lion1 cable connecting Finland and Germany and the Arelion cable linking Sweden and Lithuania (Edwards & Seidenstein, 2025). Several such incidents have occurred in Taiwan (Tyson, 2025) and the Red Sea (James, 2025), although the causes were not always determined.

The repairs of such cables cost tens of millions of euros, while the losses of economic activity and the implications of connectivity outage can have huge social and political costs (Edwards & Seidenstein, 2025). On other hand, data centres are threatened by cyberthreats as well as physical damage caused by accidents, physical phenomena like

fires[36], or even bugs. When cyberattacks or espionage are involved, it usually concerns financial or national security data (Cohen, 2024).

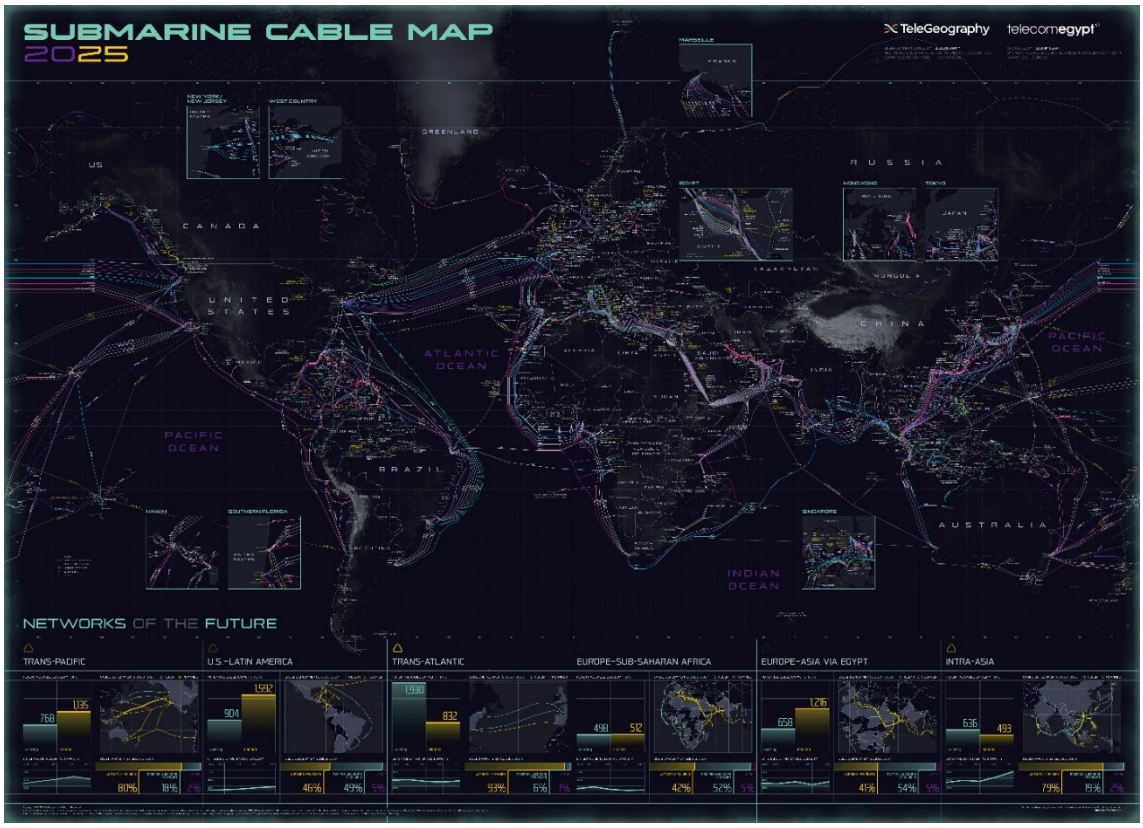

Figure 1 - Global submarine cable map 2025, Retrieved from: https://submarine-cable-map-2025.telegeography.com/

To understand the scale of this infrastructure, Figure 1 - Global submarine cable map 2025, Retrieved from: https://submarine-cable-map-2025.telegeography.com/displays a map of the global submarine cable network as of 2025. The image, however, implies the dangers posed by this level of interconnectedness, which not only touches the infrastructure, but also the supply chain it needs to exist. Data centres can be affected by conflicts concerning major hardware suppliers, like Taiwan and its semiconductor industry. Depending also on China for critical minerals exports can endanger the progress of infrastructure development, or its repair and maintenance. These are not mere considerations, but actual security risks towards economic security and strategic autonomy, as demonstrated

[36] In September 2025, government data centre in South Korea caught fire (Jung-joo, 2025).

by past events, including the 1973 Arab oil embargo or the COVID-19 pandemic. Such events should be lessons applied towards data (Cohen, 2024).

4.3 Data governance, flows and localisation

During its infant years, the internet was at large kept out of the state surveillance, censorship and any sense of control by central authorities, as it was intended[37]. As the internet and the use of data became drivers of a country's economy, as the information and digital economies grew, so did the need for state monitoring, international cooperation and ultimately governance (Jiang & Martin, 2020). The need for state-interference rose also due to the growing power of the internet's oligopoly, GAFAM[38], which earned gains and ground on the web for as long as it remained unregulated, yet the online platforms were financialised (Smyrnaios, 2018). Over the past few years, several countries have set up their own set of data governance regulations, which has political qualities with an international dimension. For one, data governance impacts the way of conduct of tech giants, affecting commercial interests by raising operational and bureaucratic costs while restraining their liberties over data use. Ultimately, this affects inter-state relations, due to the effects of data governance on cross-border data trade, strained by data localisation measures (Jiang & Martin, 2020).

In Europe, this regulatory paradigm first started quite early, with the Data Protection Directive (95/46/EC, 1995), which was later updated to what has created a global domino effect: the General Data Protection Regulation (GDPR, EU 2016/679, 2018)[39]. Both these pieces of legislation positioned the EU as the pioneer of personal data protection (Jiang &

[37] The early web community, including the world-wide web's creator, Tim Berners-Lee, had some standards for running and building the web, including decentralization, non-discrimination, bottom-up design, universality and consensus. The concept of decentralization meant at the time that www users would need no central authority's permission for their online activity, which ensured freedom from censorship and surveillance (Berners-Lee, 2009).

[38] Google, Apple, Facebook, Amazon and Microsoft.

[39] Apart from data protection in particular, the EU also sought to protect e-commerce, both consumers and traders, first with the E-commerce directive (2000/31/EC) and then with the Digital Markets Act (EU 2022/1925) and Digital Services Act (EU 2022/2065).

Martin, 2020). Margrethe Vestager[40], while nominated to become the antitrust chief for the EU, had stated that personal data is the currency of the Internet, warning of Google and Amazon's amassment of data (Kanter, 2014). The GDPR highlights the protection of personal data and emphasises individual rights, like the right to privacy. However, this regulation has long received criticism for the barriers it has caused internally and externally. First, the burden of compliance and navigation of the red-tape has increased the operational costs of European small and medium enterprises (SMEs). Second, the GDPR has had effects on cross-border trade, by restricting the transfer of EU residents' personal data outside the European Economic Area (EEA), unless the country receives an adequacy decision[41] (Jiang & Martin, 2020).

Inescapably, the EU assumed the role of the regulator on the global stance, concerning digital technologies. Coined as the "Brussels Effect", many countries around the world adapted to the GDPR, with national legislations mirroring or mimicking it, mostly for conducting trade with the EU without violating GDPR. These include Brazil, Japan, South Korea and Kenya (Treverton & Esfandiari, 2021 & European Commission, 2020). This was somewhat recognised by the Council Conclusions on EU Digital Diplomacy (2022) as a desired objective, acknowledging the Global Gateway as a means for spreading not only EU technological solutions and infrastructure investments, but also EU standards; like the GDPR. This was also in line with the EUs ability and strategic objective to capitalise on its geopolitical capital to shape foreign data governance models so that they promote EU values, like human rights protection, rule of law and democratic principles (Ricart, 2025). Figure 2 shows more countries affected by the Brussels Effect and the extent to which their regulations approximate GDPR.

[40] Former EU Commissioner for Competition and Executive European Commission Vice-President for a Europe fit for the digital age (European Commission, n.d.).

[41] This would grant that the country receiving the personal data has in place "adequate protection for individuals".

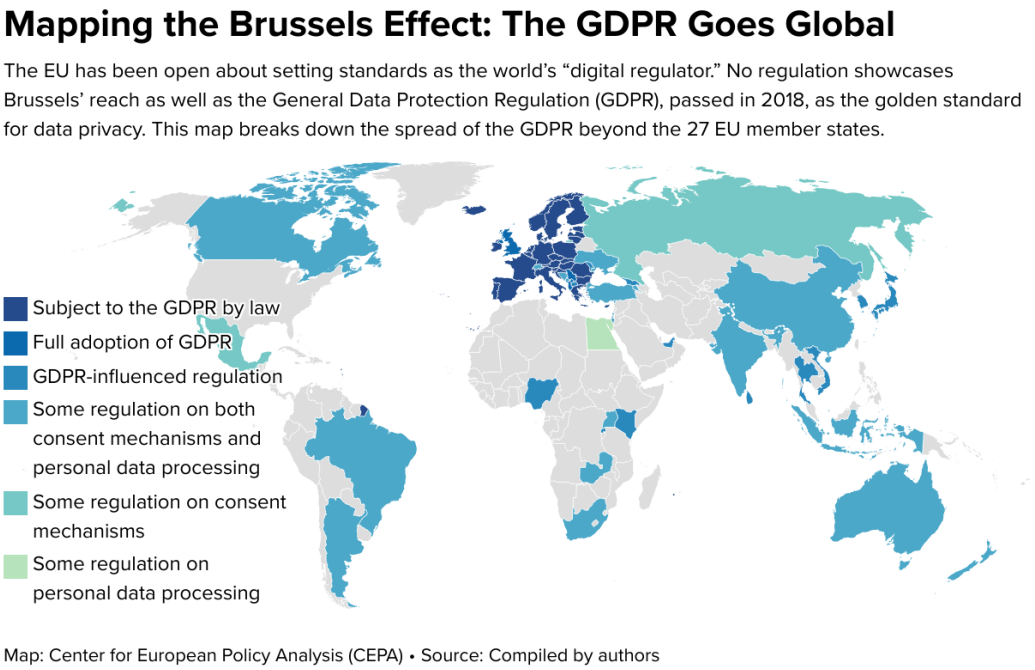

Figure 2 Mapping the Brussels Effect: The GDPR Goes Global, Retrieved from: https://cepa.org/comprehensive-reports/mapping-the-brussels-effect-the-gdpr-goes-global/

Recently, however, the EU took a step back from GDPR, a direction that was fortified by the publication of the Digital Omnibus on 19 November 2025, which is itself a response on the Draghi report (2024). This is a package of simplification measures targeting the AI act, the GDPR, cookie policies and the delayed e-privacy regulation, aiming at facilitating innovation and loosening the pressure of SMEs (Carpenter-Zehe, 2025 & Jahangir, 2025).

A year before the GDPR, in 2017, China published the Internet Cyber Security Law, a bid in the country's effort to become a leading AI operator by 2030. The Chinese position does not riddle itself with the relationship between data subject and data processor[42]. The "de facto data processor" is the state. This legislation imposing storage on local Chinese servers, restrictions on cross-border data flows for technological, economic, or scientific data (to protect national interests), and government security audits on companies' source code. The data localisation clauses of the regulation concern both outgoing and incoming

[42] Data subject is the individual who can be identified in the data, while data processor is the entity responsible for data use and handling (Jiang & Martin, 2020).

data flows, meaning that all incoming data must be stored locally, which creates a digital receipt of the transaction and opens the floor for state censorship on foreign content. This localisation of data is aimed to serve the greater goal of cyberspace sovereignty and AI innovation, which benefits from the vast amounts of data, now protected from foreign acquisition (Jiang & Martin, 2020). China has also influenced the governance models of other countries, like Tanzania, Nigeria, Vietnam and Russia (Sacks, 2018 & Jiang and Martin, 2020).

The US still holds an approach that favours economic activity and businesses, at the expense of commercialising personal data. There are approaches at state-level, like the Californian Consumer Privacy Act, which aligns to GDPR rights without mirroring it. However, this Act has also been criticised for the effect it might have if adopted nationally, enforcing restrictive regulations and strangling corporations (Jiang & Martin, 2020).

In this vein, the current US administration has largely criticised the EU on (mostly) GPDR fines imposed on large technology providers and platforms[43], like Google, Microsoft and Meta. Issued on 21 February 2025 by the Trump administration, the memorandum "Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties" targets any type of regulatory measure, including national taxes on the digital sector, the GDPR, DSA or DMA, which disproportionately[44] affect US companies[45], hinder their economic interests abroad or infringe on freedom of expression[46] (Thibout, 2025). The counter-argument here is that Europe wishes to attract rather than halt financial and technological investments, the proof coming from the European Commission's move to adopt the "adequacy decision" against the 2020 European Court of Justice ruling which characterised personal data transfers between US and EU as illegal. The adequacy decision validated US legislation as compliant with the

[43] Very large online platforms (VLOPs) or very large online search engines (VLOSEs) (European Commission, 2025)
[44] According to the memorandum. Also, out of the €5.65 billion worth of fines issued by the EU, 83 percent (€4.68 billion) was directed at US companies (Castro, 2025).
[45] Particularly, the GAFAM.
[46] This has particularly been stressed by X (former Twitter).

GDPR (Thibout, 2025). Nonetheless, the Trump administration has proclaimed tariff retaliation against these regulatory measures, deeming them a threat towards national interests, by compromising the country's strategic advantage (Castro, 2025).

Such anxieties about the strategic advantage obtained by data flows are not limited to the US. However, the US is concerned about restrictions to incoming data flows, while other governments are more focused on outgoing. This can already be observed in measures like the data governance regulations we saw in the examples of EU and China, which try to ensure that the regulation addresses also cross-border data flows. The GDPR does this by restricting the flow of personal data outside the EEA and the Chinese Internet Cyber Security Law controls both incoming and outgoing data flows. However, data flows are largely addressed by trade agreements rather than governance frameworks, as the latter are deemed to impose restrictions on trade (Leblond, 2024).

Cross-border data free flows and data localisation measures are on the opposite edges of a spectrum of policy and regulatory measures adopted globally. According to OECD data, by 2024 there were more than 100 data localisation measures on non-personal data, most of which mandate some short of governmental safeguard on the data flows, rather than completely prohibiting storage and processing outside of national borders (González, Del Giovane, & Ferencz, 2025). The increasing restrictions in data flows, both in numbers and in quality of measures, have created a fragmented landscape for businesses to navigate, thus creating friction and delays in the innovations and economic gains that data "promise"[47] (Leblond, 2024), while both the OECD (2025) and World Economic forum (2019) report the measures are becoming increasingly restrictive. The free flow of data internationally was projected to contribute $11 trillion to the global GDP, surpassing the global trade in goods (Basu, 2025). Data flow restrictions are estimated to counter this trend, inflicting also costs in virtually any economic sector, digital or not, as well as research, academia and the civic space (World Economic Forum, 2017).

[47] This refers to the multiple policy documents and commentative articles which have elevated data to be the foundation, "lifeblood" and driver of the digital economy, ultimately acknowledging data as a resource of strategic importance for the realisation of national interests.

The politics behind these restrictions in data transfers are not only a choice for the protection of personal data and human rights, rather shaped by power asymmetries and the subsequent need for control over an important resource. Data localisation measures aim to restrict transfer and storage of data outside of a country's borders, with the aim of protecting personal data from foreign access, but also any domestically produced data, to enhance national technological advantage (Jiang & Martin, 2020). Apart from the economic value that data have, especially in the face of emerging technologies like AI, there are other national interests served by data localisation. For example, geolocation, trade, health, climate and other data are deemed important for national security interests (Basu, 2025), while personal data that facilitate behavioural analytics can open the doors to foreign interference (Ndemo, 2024 & Council of the European Union, 2023).

4.4 Data sovereignty

Data sovereignty is a cross-cutting issue, touching on infrastructure, security and governance, although they are also tightly connected to one another, too. The tendency to safeguard data into a country's own borders is tightly connected with the significance of data and the risks entailed by the apparent oligopoly of control, not only on data, but also the infrastructure necessary for storage, transmission and processing. These risks pertain to governmental controls by the two leaders of the sector, US and China, but also by the commercial interests of the private elite which dominates the field over the state.

Data sovereignty entails state control over data generation, storage, processing, and transmission within national borders and involving national entities (Ezenwaka, 2025). Linking to the chapters on infrastructure and security, Europe's position within this context highlights the strategic paradox of regions dependent upon US technological infrastructure. A leading Belgian cybersecurity official has articulated the uncomfortable reality: Europe has "lost the Internet", since it is entirely dependent on US tech giants for most of its digital infrastructure. Storing data exclusively on European soil has become is impossible. These companies also have, naturally, only commercial interests in mind, which can easily turn against state interests or be used for even greater gains. Europe's

loss of technological autonomy in these critical domains represents not merely an economic disadvantage but a security compromise of considerable magnitude (In.gr, 2026).

Data sovereignty falls under the scope of digital sovereignty, now a cornerstone of national security strategy, which covers the topics of infrastructure, governance and capabilities (Ezenwaka, 2025). Since building sovereign infrastructure takes large investments and time, regulatory and policy measures have been given priority. Data localisation policies serve the greater objective of data sovereignty, by protecting domestically generated data from foreign control, while providing the opportunity for the data sovereign to use the data without delays, obstructions or prohibitions. Although there is no consensus on the meaning of this term, it suggests the exercise of control of generation, storage, processing and transfer of data within national borders, against foreign transfers and uses (Ezenwaka, 2025). In addition, the European Strategy for Data aims for data sovereignty, via creating a single market for data, which would also enhance competitiveness. A step to that direction is the creation of Common European Data Spaces, pools of European data available for economic and societal purposes, directed at exerting some level of control over data generators, individual and commercial alike (European Commission, 2020). However, the dominance of GAFAM over data in every aspect (European Commission, 2020) is an impediment to real sovereignty. As per Lehdonvirta, "*If sovereignty has to be bought as a service, is it really sovereignty*"? This oligopoly of tech giants puts any state actor at risk of the whims of private individuals.

4.5 The consequences of datafication on diplomacy

This paper has shown so far that behind most aspects of digital technology hides data, a position backed by papers and statistics. However, the level this position is true surpasses the study of diplomacy itself and all the factors which affect international relations and enters the sphere of human experience. The technological revolution we have been seeing for the first quarter of the 21st century has brought people life conveniences ranging from gadgets, smart devices, digital social networks, all of which are mobile data

collectors and transmitters, feeding from and back to the human experience. To top it all off: there is no alternative, as daily life has become inescapably connected to virtual products and processes.

This has created an evergreen supply chain of personal data shared at people's own free will, which then feed an "interface" of behavioural analysis and personalisation of the content (more data) received. Initially this interface loop and its products were not directed at the users, but for businesses to use the insights to attract more customers and better sales. However, there are concrete examples that this "datafication" of the human experience has already been turned against humans (Zuboff, 2019).

Digital technology behemoths claim data as property, based on the notion that was described earlier in the paper where the consumer becomes the product if the experience is free. With data ownership, comes ownership over the value produced. Considering the volume and variety of data produced in the last decade alone, the value is unmatched to what insights it provides of the human neuropsychology (Zuboff, 2019). In Zuboff's handbook, this is called surveillance capitalism, under which tech giants, like Google and Facebook (parents of the phenomenon), have more data on citizens than governments do. This raises a range of issues, from violation of privacy, to manipulation for economic gains, to the total restructuring of societal norms and economic relations. But how does this particularly impact diplomacy? The effect can be two-fold, at least.

On the one hand, surveillance capitalism is connected with the geopolitics of information. Once Google and Facebook started feeding the products of behavioural insights back to the users of their platforms, the scales shifted; tech giants were not only monitoring and analysing human behaviour, but were now using their insights to configure it (Zuboff, 2019). At first this might have had business intents, but the Cambridge Analytica showcased how users' online data can capitalise on human experience to render said human a target for political objectives (Cadwalladr & Graham-Harrison, 2018). Behavioural customisation was studied from Facebook back in 2012-2013, when a company experiment demonstrated that it is possible to apply subtle messaging which

transcends human awareness, to actually modify behaviour and emotion of platform users (Zuboff, 2019). These findings are very much in line with the polarising effects algorithms have been proven to have on social media users (Lloyd, 2025).

This datafication has cultivated the way to fake news and political manipulation of information, which can be a diplomatic issue in the case of foreign interference. This type of power of information and the manipulation thereof is considered strategic from governments, not only for internal use, but also in the context of foreign interference and information manipulation[48] (FIMI) (Zuboff, 2019 and Rosenbach & Mansted, 2019). According to Rosenbach and Mansted (2019), Keohane and Nye identified three types of information: free, commercial and strategic, which have all turned out to be of strategic importance to state actors. This connects back to the geopolitics of information. States share the tech giant's interest in acquiring personal information about citizens, particularly information that can reveal behavioural characteristics with the goal of influencing thought and action patterns. This is not only used by domestic actors, but also foreign ones, like Russia's interference in the 2016 disinformation campaign during the presidential election, targeting citizens most vulnerable to polarisation. AI and advanced computing will exacerbate this trend, leading to "information statecraft" (Rosenbach & Mansted, 2019).

Narendra Modi, the Indian Prime Minister, has stated that acquisition and control over data can create a hegemon, particularly through engraving one's culture and ideology across the world (Rosenbach & Mansted, 2019). In other words, whoever controls the data, controls the information and thus the narrative, which would be a major win for digital (public) diplomacy. This control over data, regardless of handling the narrative or not, has largely led to data localisation measures, which apart from aiming to boost data-driven innovation, they also strive to protect domestic data from foreign manipulation. The significance of these protective measures becomes clearer with the case of data

[48] Countering FIMI is one of the objectives of the Council Conclusion on digital diplomacy (Council of the European Union, 2023), specifically referencing the context of the Russian war of aggression against Ukraine.

tampering of decision-assistance systems. If the foundational data of the system is "poisoned", so will be the outcome, inflicting another hit against a foreign government[49] (Rosenbach & Mansted, 2019).

Another aspect which will affect diplomacy pertains to the increasing volume of data and the potential for mal-intended influence on formal diplomacy, inflamed by AI and its potential for both fast data processing and data generation (images, videos, text etc.). However, this will not only have negative side effects, in terms of overwhelming track I diplomacy in dealing with such hybrid and novel challenges, but also positive ones. The proliferation of data analytics and data science, combined with the emerging technologies and computational power can provide diplomats with ample opportunities, as outlined in the studies over data diplomacy, where data is considered a tool to extract insights and generate knowledge and intelligence (see chapter 2.1 "Data in diplomacy") (Treverton & Esfandiari, 2021).

On the other hand, the effects of surveillance capitalism on diplomacy are not related to the *information* controlled by the phenomenon. The danger lies in *who* controls the information. This phenomenon has led to a concentration of information and knowledge to an elite of private owners who can profit off of sharing information at will (Rosenbach & Mansted, 2019). Not only does the dominance of private tech corporations cause issues of sovereignty over data, but it births an entire new agent with which diplomacy needs to converse, negotiate and come to agreements with for a series of topics around the ownership data, critical infrastructure, vital software and dominance of the cyberspace. Diplomacy here will not have to deal only with cross-border diplomatic relations, but immerse into a new terrain of diplomatic relations between private and public sphere, which so far looked more like business transactions. With the growing power of the GAFAM and their likes, owing to property rights of critical assets of public goods, the relationship will change and the private sector will potentially hold the upper hand.

[49] An example here presented by Rosenbach and Mansted (2019) is the Stuxnet malware attack against the Iranian Natanz nuclear plant, which infected the plant's computers controlling nuclear centrifuges.

Once again, state sovereignty is at stake in this scenario.

5 Discussion

Data diplomacy encompasses an understanding of how data shape the international affairs landscape and affect diplomatic practice. The data revolution has flooded the arena with developments on every front: regulation, governance, critical infrastructure and supply chains, security thereof and cybersecurity. It has also cultivated the field for an era of information geopolitics, with consequences on state-citizen and inter-state interactions (Rosenbach & Mansted, 2019). Focusing on the latter, data diplomacy not only faces this development, in conjunction to all other identified challenges, but must synthesise intelligence based on this data interdependence of all these seemingly different areas, which are so far treated in silos. Diplomacy must adapt to new ways of defining and understanding national interests and strategic priorities, to decipher all the power plays.

5.1 Global sphere

When looking at the big picture, the data-diplomacy interactions are driven largely by the two poles of antagonism, US and China. From chip wars to sanctions and tariffs, the two countries aim at becoming the technology hegemon, and they have the means to do so. Each of them dominates a particular piece of the puzzle. The US is leading in data centre infrastructure, semiconductor development and advanced AI models, driven by virtually no regulatory restrictions, economic favours to tech giants and the use of economic coercion to other countries, even allies, to maintain authority over data inflows. On the other hand, China dominates the supply sector of critical minerals and rare earths, which are necessary for data-related hardware and infrastructure, as well as clean energy. On the latter, China is also a leader, which provides a strategic advantage due to less dependency on fossil fuels. Although the US is host to more data storage units and companies who can exploit them, China has steadily built a network of infrastructure projects across Asia, Africa and Europe, via the Belt and Road Initiative (BRI) and its branch, the Digital Silk Road (DSR) (Council on Foreign Relations, n.d.), which has expanded in Latin America, too (McBride, Berman, & Chatzky, 2023). Through such

investments, China gets tied to the receiving countries with strategic interests, developing economic interdependence and gaining geoeconomic influence. Consequently, the country can exert influence over the data governance models of its partners as well, paving the way for easier data flows between them (Esposito, 2025). More than 130 countries are involved in projects under the BRI (Council on Foreign Relations, n.d.), highlighting China's instrumentalization of data diplomacy to safeguard a position amidst geopolitical technology competitions.

Similar to the influence China has across continents, Europe has achieved a domino effect over data governance regimes world over, with the GDPR since 2018. European trade partners with strong bonds have adapted their regulatory environment to comply with Europe, creating gains for both parties via unhindered commercial relations. The US shifted its stance on data provisions in free trade agreements (FTAs) after 2023. From supporting free flow of data and objecting data localisation measures and federal data regulation, the Biden administration reassessed those stances, in promoting some level of data (Trachtenberg, 2025). Today, the stance on such measures is not entirely clear, although the Trump administration has been very vocal about how EU regulatory measures over data discriminate against US tech giants, calling for retaliatory steps.

To counter the effects of the BRI, Europe built on the Global Gateaway strategy, "greasing" its position to project geopolitical power, particularly over Africa, while aiming at increasing its strategic advantage over natural resources necessary for data critical infrastructure. By opening up towards Africa with infrastructure projects, Europe is trying to diversify its market access and resources, to loosen its dependence on the US, while countering Chinese influence on the African continent. Policy officials and AI experts have repeatedly expressed the need to develop autonomy and sovereignty over data itself and the resources that support the data and AI ecosystem. Yet, the Global Gateaway combines infrastructure investments with Europe's "normative power" (Noureddine, 2016). The agony over supply chain security (autonomy) and data sovereignty is shared not only by the three major global players, but also by every state, in light of the increasing weaponisation of strategic advantages. Europe also has the capacity to play the game of

geoeconomic coercion, without showcasing the willpower. From the SWIFT system (based in Belgium), to European companies that can dominate the infrastructure competitions, like the semiconductor lithography giant ASML (Dutch) and 5G provider Ericsson (Swedish) Europe has access to a few chokepoints that can be instrumentalised for greater geopolitical and technological gains (Farrell & Newman, 2025).

Paradoxically, there has not been a coordinated approach towards data flow regulations or trade agreements with provisions on digital and data trade from international institutions, like the World Trade Organisation (WTO) or the United Nations (UN); at least, not to address the increasing antagonism. Institutionalisation of data diplomacy has made an appearance in dealing with notions of democracy, human rights, global sustainable development. Even the UN Global Compact does not concern state relations per se, rather overarching topics requiring attention and cooperation in view of the rapid digitalisation (United Nations, 2024). Therefore, international diplomatic spaces have not publicly mobilised to address the shifting geopolitics. Any and all diplomatic relations happen on a bilateral level between the main poles of power and conflict, or regionally. Europe has institutionalised bilateral dialogues, through the EU-US Trade and Technology Council, the EU-India Trade and Technology Council, the Digital Partnership Agreements with many Indo-Pacific countries -Japan, Republic of Korea, and Singapore-, the launch of the EU-LAC Digital Alliance, or the strengthening of the Digital Agenda for Western Balkans (Ricart, 2025).

5.2 Regional neighbourhood

While the global layer showcases conflict and plays a zero-sum game, at a regional level cooperation drives foreign relations. This is observed via bilateral cooperation examples emerging as regional digital hubs, existing regional organisations signing new agreements, or alliances under new topics. The objective plays along the lines of sovereignty and strategic autonomy, at least against the two competing powers.

The Association of Southeast Asian Nations (ASEAN) is negotiating the Digital Economy Framework Agreement (DEFA), the first-of-its-kind regional agreement focused on digital economy governance, with explicit provision on data flows and harmonisation measures, to boost the digital economy in the region by removing regulatory friction (Feingold & Pfister, 2026). In the midst of competing regulatory frameworks and fragmented approaches, while data rules in FTAs are spreading, the DEFA will provide an advantage to the region, let alone set an example for regional agreements in the future (Lee, 2023). On the other hand, the "Chip 4" alliance between US, Japan, Taiwan and South Korea aims at promoting the countries' strategic interests in the semiconductor industry, ultimately promoting supply chain security and data infrastructure profits (Esposito, 2025).

On a bilateral level, yet creating a regional hub for data and AI dominance, the France–UAE partnership illustrates how data diplomacy risks lead to new opportunities. Both countries are leaders in their respective regions and have aligned their national AI strategies within a broader geopolitical vision that merges digital innovation with strategic influence. The partnership operates not as a technological collaboration but as an exercise in strategic foresight, reflecting how states increasingly leverage AI to shape international norms, enhance sovereignty, and secure long-term competitiveness. France's focus on digital sovereignty and infrastructural autonomy complements the UAE's ambition to emerge as a global AI hub, leading to a symbiotic relationship embedded in shared objectives of innovation, investment, and talent development. The establishment of Europe's largest AI campus in Île-de-France, co-financed by Franco–Emirati actors, underscores how bilateral cooperation can transcend national interests to produce strategic assets with global effects. In this context, data diplomacy becomes both a manifestation of state power and a new modality of foreign policy, demonstrating how data-driven technologies redefine influence and partnership in the international system (Karacsony, 2025).

Exploring the regional power dynamics in other geographies should be a topic for further research, to identify how this pattern of cooperation appears or not in other different regions.

5.3 Recommendations: A place for data diplomacy

The challenges that data pose to international relations have been examined in this paper to demonstrate how and why data function as an essential and strategic national resource, a resource that increasingly shapes international relations, foreign policy, and diplomacy, through sifting geopolitics. The key issue is not whether a new concept is required to merge data and tech diplomacy, but rather how the existing notion of data diplomacy should be conceptualised, studied, and implemented in practice. Most importantly, the discussion should focus on why data diplomacy needs to take a more central role in foreign policy decision-making. The distance between academic articles, policy papers, reports, and media analyses are bridged in this paper, by offering a comprehensive perspective on the intersections between data, international relations, and diplomacy, through key issues like security, interdependence, geopolitics, infrastructure and privatisation even.

To face the challenges of an ever-digitalised global environment and economy, diplomatic actors must cultivate a deep understanding of data, its value, potential as a resource, and the broader ecosystem in which it exists, encompassing infrastructure, regulation, and culture. Given the significance of data as a resource, a solid foundation of knowledge on data, its movement and supporting infrastructure will provide diplomats and foreign policy analysts with a bold perspective of current affairs. Insights is what supports decision making and better negotiations. While data is a tool supporting the extraction of insights and intelligence, acknowledgment needs to come on how data should be the item getting intelligence on. This paper has showcased that a series of foreign policy topics are interconnected with building the capacity to transfer, use and store data, thus such a topic needs to be embedded in diplomatic agendas around technology, critical infrastructure, international partnerships and securing of resources. Data diplomacy involves identifying trusted international partners, mobilising public and private capital, addressing data security and privacy risks, and fostering innovation across the technological landscape. The field has become both an urgent necessity and a promising avenue for collaboration. Successfully navigating the geopolitics of the data era will demand stronger partnerships between public institutions and private enterprises. While not every state will emerge as

a global leader in artificial intelligence, leadership need not be confined to only the United States or China. For the United States in particular, its competitive advantage will depend on leveraging its network of global alliances and partnerships across sectors, instead of the antagonistic stance it currently holds. In Europe, the situations differs and the necessity for developing strategic autonomy becomes more pressing as the world moves further into the second year of this Trump administration.

Given the growing weight of data in the global balance between competition and competition, several policy and institutional measures should be prioritised to ensure that data diplomacy evolves in a manner consistent with the needs of diplomats and the demands of this emerging era.

States need to diversify their portfolios concerning supply chains, trade deals, alliances, not only concerning the data value chain, but also other critical goods and infrastructure, like energy and minerals for other sectors. These seemingly go into the territory of trade policy. However, diplomatic efforts are needed to ensure that new partnerships are secured and that a state's foreign relations and standing on the international stage remain secure in the face of growing competition, AI rivalries and weaponised economy. This diversification will allow state actors to protect themselves from coercion or retaliatory measures, central themes of recent foreign relations (Platias & Constantopoulos, 2025). Emerging technology alliances, such as the France-UAE partnership and ASEAN's regional agreements examples show that collective strength and middle technology powers[50] can play a key role in shaping the regional and global landscape. These can be an early example to guide new cooperative frameworks involving governments, civil society, and private sector actors can create shared rules for data exchange and innovation, preventing the weaponisation of data as a tool of coercive action. Building new and diverse partnerships is another branch of diversifying the state portfolio and mitigating the vulnerabilities of dependence on fickle sources of power and stability.

[50] Considering that US and China are the great tech powers, by the standard of means, capacity and influence in the geopolitics of it.

In the same vein, European leaders need to be steady concerning the Union's autonomy in technology, data and AI. Investments have been announced by the European Commission, reaching billions of euros (Chee, 2025), profiting several EU based companies, like ASML and Mistral. Such investments need to be protected from other countries' foreign policy whims and disruptions in the supply chains of energy, minerals, hardware and data flows. Europe needs to ensure stability in the data value chain, so that such investments will have the expected returns. Decision makers should also understand better the complexities of data transfers and have a clearer view of contradicting pieces of legislation. This pertains to the localisation measures of data centres. As Europe moves forward with investments on data centres located in member states, most of these facilities are in cooperation with US tech giants, like Google and Amazon (AWS[51]). Apart from the reliance this creates on the US (Nicol-Schwarz, 2026), increasing risks for European data security. Therefore, diversification goes hand in hand with investments "in-house".

Another step to increasing security and resilience of data ecosystems would requires countries to follow the example of Estonia's data embassy. Estonia started with an agreement with Luxembourg to host a data centre with the most important state datasets to protect the country's continuity through data preservation (e-Estonia, 2019). Investing in transparency and resilience of data ecosystems through such smart infrastructure could lead to strengthened collaboration regionally and higher mitigation of several security risks, including cyberthreats or natural hazards. Countries should further adopt data resilience strategies that protect against manipulation, disinformation, and infrastructure attacks. Diplomacy can pursue public-private partnerships to enhance data integrity and the public sector's capacity to fend off foreign interference and security threats related to data leaks and manipulation.

[51] Amazon Web Services

6 Conclusions

Diplomacy has never had a linear course, yet in recent years it seems to have entered even more turbulent waters. The convergence of technological disruption, growing multipolarity and the weaponisation of economic interdependence has created a landscape in which the rules are rewritten faster than institutions can adapt. Data sits at the centre of this turbulence, not as a peripheral concern of the digital age, but as a strategic resource shaping the terms on which states compete, cooperate and ultimately survive.

Data diplomacy is rapidly reshaping the geopolitical and normative landscape of international relations. As states seek to assert influence in the digital domain, data has become both a strategic resource and a diplomatic currency. As a resource, it fuels AI development, informs military strategy, powers surveillance, and drives economic growth. As a currency, it is traded, withheld, leveraged, and weaponised in bilateral negotiations, trade agreements, and infrastructure deals. The international system is increasingly defined by asymmetries in technological capacity, data access and regulatory influence. Great powers now pursue hegemony not through territorial conquest, but through control over data infrastructures, AI capabilities, and digital ecosystems that underpin economic, strategic, and military advantage.

Yet data interdependence also creates a paradox: the same networks that enable strategic competition demand cooperation to remain functional. No state, however powerful, can claim full sovereignty of the data value chain, ranging from chips, cables, cloud infrastructure, and critical minerals. Initiatives such as the EU's Global Gateway and China's Digital Silk Road reflect competing efforts to establish spheres of influence and expand their reach into valuable resources, but int the end it all depends on stable, interoperable data exchanges to deliver value. US and Chinese export restrictions hurt both sides. European data sovereignty ambitions remain constrained by reliance on American cloud infrastructure. This complex balance between rivalry and collaboration

defines the new diplomatic environment, and it is one that punishes purely antagonistic stances.

To navigate this environment, states must move beyond reactive strategies and develop proactive, value-based models of data diplomacy. For Europe in particular, this means turning dormant assets into deliberate strategy. Synergies among EU-based companies and between them and Member State governments, illustrated by cases such as Mistral AI and Greece's new deal, should be actively fostered to build a coherent European data ecosystem, neither dependent on nor exposed to US and China. Equally, the Global Gateway must be wielded with strategic discipline as a vehicle for durable partnerships through trade deals and infrastructure projects that embed European standards and generate genuine returns, countering Chinese expansion without unnecessary escalation.

The ball is in the court of the state. Private actors have accumulated extraordinary leverage over digital infrastructure, data flows, and AI capabilities, and they will continue to do so. But the frameworks within which they operate, the alliances that give them reach and the norms that constrain or enable their behaviour remain political choices. States that abdicate this responsibility, outsourcing data governance to market forces or retreating into digital isolationism, will find themselves overpowered in the next phase of geopolitical competition. Those that invest in diplomatic capital, build coalitions around shared values, and develop the institutional literacy to engage with the data layer of international relations will be better positioned to shape what comes next.

Ultimately, the future of diplomacy in the data age will depend on the capacity of states and institutions to align technological innovation with democratic accountability. This paper has argued that data diplomacy should not be treated as a niche subfield or a technical afterthought, but as a strategic lens through which the evolving contest for power in the 21st century must be read.

7 References

Adesina, O. S. (2017). Foreign policy in an era of digital diplomacy. *Cogent Social Sciences*. doi:10.1080/23311886.2017.1297175

Ahmed, S. (2025, February 17). *The Geopolitics of Energy: How oil and Gas Shape Diplomacy*. Retrieved December 2025, from Modern Diplomacy: https://moderndiplomacy.eu/2025/02/17/the-geopolitics-of-energy-how-oil-and-gas-shape-diplomacy/

Alaamer, K. (2025, April 22). *This is the state of play in the global data centre gold rush*. Retrieved from World Economic Forum: https://www.weforum.org/stories/2025/04/data-centre-gold-rush-ai/

Allison, G., Klyman, K., Barbesino, K., & Yen, H. (2021). *The Great Tech Rivalry: China vs the U.S.* Harvard Kennedy School, Belfer Center for Science and International Affairs, Cambridge, MA.

Ambler, S. W. (n.d.). *A Metaphor for Data Quality: Data is the New Water*. Retrieved January 2026, from AgileData.org: https://agiledata.org/essays/data-quality-metaphor.html

APEC. (2020). *APEC Guidelines and Best Practices for the Adoption of Global Data Standards*. Retrieved from APEC: https://www.apec.org/publications/2020/03/apec-guidelines-and-best-practices-for-the-adoption-of-global-data-standards

Arthur, C. (2013, August 23). *Tech giants may be huge, but nothing matches big data*. Retrieved from The Guardian: https://www.theguardian.com/technology/2013/aug/23/tech-giants-data

Ashton, C., & Forder, S. E. (2024, February 14). *Why data isn't the new oil anymore*. Retrieved from BCS - The Chartered Institute for IT: https://www.bcs.org/articles-opinion-and-research/why-data-isn-t-the-new-oil-anymore/

Basu, A. (2025, May 13). *Data Diplomacy: Rethinking Cross-Border Data Flows for a More Equitable Global Digital Economy.* Retrieved 2025, from Newamerica.org: https://www.newamerica.org/planetary-politics/blog/data-diplomacy-rethinking-cross-border-data-flows-for-a-more-equitable-global-digital-economy/#:~:text=The%20free%20flow%20of%20electronic,national%20power%20to%20surveil%20citizens.

Baylis, J., Smith, S., & Owens, P. (2011). *The Globalisation of World Politics* (5th ed.). Oxford University Press.

Belt and Road Portal. (n.d.). *Projects*. Retrieved 2026, from Belt and Road Portal: https://eng.yidaiyilu.gov.cn/project

Berners-Lee, S. T. (2009, October 18). *History of the Web*. Retrieved January 2026, from World Wide Web Fondation: https://webfoundation.org/about/vision/history-of-the-web/

Bou, E. (2025, March 20). *The Digital Gold Rush: Why Investors Back Sustainable Data Centres*. Retrieved 2026, from Forbes: https://www.forbes.com/sites/elenabou/2025/03/20/the-digital-gold-rush-why-investors-back-sustainable-data-centres/

Boyd, A., Gatewood, J., Thorson, S., & D. V. Dye, T. (2019, May). Data Diplomacy. *Science & Diplomacy, 8*(1). Retrieved July 2025, from http://sciencediplomacy.org/article/2019/data-diplomacy

Breuninger, K. (2025, December 8). *Trump greenlights Nvidia H200 AI chip sales to China if U.S. gets 25% cut, says Xi responded positively*. Retrieved January 2026, from CNBC: https://www.cnbc.com/2025/12/08/trump-nvidia-h200-sales-china.html

Cadwalladr , C., & Graham-Harrison, E. (2018, March 17). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. Retrieved January 2026, from The Guardian:

https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Carpenter-Zehe, O. (2025, November 20). *The Digital Omnibus has arrived — and here's what it really changes*. Retrieved January 2026, from Euobserver: https://euobserver.com/digital/areee4d315

Castro, D. (2025, April 17). *Europe's GDPR Fines Against US Firms Are Unfair and Disproportionate*. Retrieved January 2026, from Center for Data Innovation: https://datainnovation.org/2025/04/europes-gdpr-fines-against-us-firms-are-unfair-and-disproportionate/

Chari, D. S. (2025, February 14). Power, Pixels and Politics: The Geopolitics of Emerging Technologies in the Digital Age. *London Journal of Research in Humanities & Social Science, 25*(2), 1-99. Retrieved 2025, from https://journalspress.com/power-pixels-and-politics-the-geopolitics-of-emerging-technologies-in-the-digital-age/

Chee, F. Y. (2025, February 11). *EU's AI push to get 50 billion euro boost, says von der Leyen*. Retrieved from Reuters: https://www.reuters.com/technology/artificial-intelligence/eus-ai-push-get-50-bln-euro-boost-eus-von-der-leyen-says-2025-02-11/

Cohen, J. (2024, October 28). *The Next AI Debate Is About Geopolitics*. Retrieved from Foreign Policy: https://foreignpolicy.com/2024/10/28/ai-geopolitics-data-center-buildout-infrastructure/

College Hive. (n.d.). *Types of Diplomacy*. Retrieved January 4, 2026, from College Hive: https://collegehive.in/docs/3rd_sem/site/IR/Unit%20-3%20International%20Peace%20and%20Security/3.4%20types%20of%20diplomacy.html#3-environmental-diplomacy

Council of the European Union. (2023). *Council conclusions on EU Digital Diplomacy.* Brussels. Retrieved 2025, from https://www.consilium.europa.eu/en/press/press-

releases/2022/07/18/eu-digital-diplomacy-council-agrees-a-more-concerted-european-approach-to-the-challenges-posed-by-new-digital-technologies/

Council on Foreign Relations. (n.d.). *Assessing China's Digital Silk Road Initiative*. Retrieved 2026, from Council on Foreign Relations: https://www.cfr.org/china-digital-silk-road/

Cukier , K., & Mayer-Schonberger, V. (2013, April 4). Big Data: An Interview with Kenneth Cukier and Viktor Mayer-Schonberger. (S. Tobias, Interviewer) Retrieved December 2025, from https://www.cfr.org/blog/big-data-interview-kenneth-cukier-and-viktor-mayer-schonberger

Deakins, S. (2017, October 12). *Data Is The New Water: Seven Reasons Why*. Retrieved from HuffPost: https://www.huffingtonpost.co.uk/stjohn-deakins-195/data-is-the-new-water-sev_b_18228184.html

DiploFoundation. (2017). *Data Diplomacy: Mapping the field, Summary Report of the Geneva Data Diplomacy Roundtable.* Geneva: DiploFoundation. Retrieved 2025, from https://www.diplomacy.edu/wp-content/uploads/2017/08/DataDiplomacyreport.pdf

DiploFoundation. (n.d.). *Oil diplomacy*. Retrieved 2026, from Diplomacy.edu: https://www.diplomacy.edu/topics/oil-diplomacy/

DiploFoundation. (n.d.). *Types of Diplomacy*. Retrieved from diplomacy.edu: https://www.diplomacy.edu/topics/types-of-diplomacy/

DiploFoundation. (n.d.). *Water Diplomacy*. Retrieved from diplimacy.edu: https://www.diplomacy.edu/topics/water-diplomacy/

Draghi, M. (2024). *The future of European competitiveness.* Luxembourg: Publications Office of the European Union. Retrieved from https://commission.europa.eu/topics/competitiveness/draghi-report_en#paragraph_47059

D'Souza, C. (2025, December 16). *PIMCO closes record-breaking European data center fund*. Retrieved 2026, from PERE: https://www.perenews.com/pimco-closes-record-breaking-european-data-center-fund/#:~:text=PIMCO%20is%20targeting%20an%20IRR,earliest%20backers%2C%20per%20PERE%20data.

Duarte, F. (2025, April 24). *Amount of Data Created Daily (2025)*. Retrieved 2026, from Exploding Topics: https://explodingtopics.com/blog/data-generated-per-day

Dzigal, N., Safarpour, D., Godolja, D., & Susslin, L. (2025). *Digital Sovereignty and Geopolitics in the Field of Data Protection: A Comparison of the EU, China, and the USA.* Vienna. doi:10.13140/RG.2.2.29957.87522

Edwards, C., & Seidenstein, N. (2025). *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure.* International Institute for Strategic Studies. Retrieved January 2026, from https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/

e-Estonia. (2019, December 19). *Data Embassy – the digital continuity of a state*. Retrieved from e-Estonia: https://e-estonia.com/data-embassy-the-digital-continuity-of-a-state/

Einhorn, G., & King, D. (2025, October 10). *The $3.3 trillion climate question: Can data centres take the heat?* Retrieved 2026, from World Economic Forum: https://www.weforum.org/stories/2025/10/data-centres-3-3-trillion-question-heat-cooling/

Esposito, M. (2025, July 24). *AI geopolitics and data centres in the age of technological rivalry*. Retrieved from World Economic Forum: https://www.weforum.org/stories/2025/07/ai-geopolitics-data-centres-technological-rivalry/

European Commission. (2020, February 19). A European strategy for data. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL*. European Commission.

European Commission. (2025, December 12). *DSA: Very large online platforms and search engines*. Retrieved from Shaping Europe's Digital Future: https://digital-strategy.ec.europa.eu/el/policies/dsa-vlops

European Commission. (n.d.). *Margrethe Vestager*. Retrieved January 2026, from Commissioners.ec.europa.eu: https://commissioners.ec.europa.eu/margrethe-vestager_en

Eurostat. (2025, December). *Digital economy and society statistics - households and individuals.* Retrieved from Eurostat - Statistics explained: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Purpose_of_using_the_internet

Ezenwaka, C. P. (2025). Digital sovereignty and the use of competitive intelligence to understand the race for technological dominance. *International Journal of Science and Research Archive, 17*(1), 459-471. doi:https://doi.org/10.30574/ijsra.2025.17.1.2774

Farrell , H., & Newman, A. (2025, August 19). The Weaponized World Economy - Surviving the New Age of Economic Coercion. *Foreign Affairs*. Retrieved 2025, from https://www.foreignaffairs.com/united-states/weaponized-world-economy-farrell-newman

Farrell, H., Newman, A., & Wallace, J. (2022, September-October). Spirals of Delusion: How AI distorts decision-making and makes dictators more dangerous. *Foreign Affairs, 101*(5), pp. 168-181. Retrieved January 2026

Feingold, S., & Pfister, A.-K. (2026, January 5). *ASEAN takes major step toward landmark digital economy pact*. Retrieved 2026, from World Economic Forum:

https://www.weforum.org/stories/2025/10/asean-defa-digital-economy-pact-negotiations/

Fleury, M., & Jimenez, N. (2025, July 10). *'I can't drink the water' - life next to a US data centre*. Retrieved January 2026, from BBC: https://www.bbc.com/news/articles/cy8gy7lv448o

Fumega, S. (2024, November 12). *The Global Landscape of Data Governance*. Retrieved January 2026, from CIGI: https://www.cigionline.org/articles/the-global-landscape-of-data-governance/

Gandhi, H., & Chandran, R. (2025, December 15). *We mapped the world's hottest data centers*. Retrieved from Rest of the World: https://restofworld.org/2025/data-center-heat-map/

González, J. L., Del Giovane, C., & Ferencz, J. (2025). A Preliminary Mapping of measures affecting Cross-Border Flow of Non-Personal Data. *OECD Trade Policy Papers*(No. 295). doi:https://doi.org/10.1787/0825c57c-en.

Goodson, S. (2012, March 5). *If You're Not Paying For It, You Become The Product*. Retrieved from Forbes: https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/

Hartshorn, J. E. (1973, July). Oil Diplomacy: The New Approach. *The World Today, 29*(7), pp. 281-290. Retrieved 2025, from https://www.jstor.org/stable/40394710

Hinrich Foundation and Visual Capitalist. (2025). *The Age of Data.* Hinrich Foundation. Retrieved 2025, from https://www.hinrichfoundation.com/research/infographics/age-of-data?utm_campaign=wp-vc-age-of-data&utm_medium=email&_hsenc=p2ANqtz-8Bejx7G1vNKgrE9Ud-ZBZ6WEqJa2Pq2GSmDjlV2miejonzbxPvObaUljfWkuQBnS9sfy9ih85kc1hGeN2zPA6Jg4WpLvaVNFDYVyW6L-G-taPDhRE&_hsmi=3897

Hodgson, C. (2025, December 21). *"Eldorado" in the copper market caused by data centres*. Retrieved 2026, from Euro2Day: https://www.euro2day.gr/ftcom/ftcom_gr/article-ft-gr/2328456/elntoranto-sthn-agora-halkoy-fernoyn-ta-data-cente.html

In.gr. (2026, January 2). *Europe has lost the internet war, warns cybersecurity official*. Retrieved January 2026, from In.gr: https://www.in.gr/2026/01/02/in-science/technology/eyropi-exase-ton-polemo-tou-diadiktyou-proeidopoiei-aksiomatouxos-kyvernoasfaleias/

Inteliment. (2024). *Data is NOT Oil – Data Is the New Soil*. Retrieved from Inteliment.com: https://inteliment.com/industries/data-is-not-oil-data-is-the-new-soil/

International Data Spaces Association. (n.d.). *International standards*. Retrieved 2025, from International Data Spaces Association: https://internationaldataspaces.org/why/international-standards/

International Telecommunication Union, Development Sector. (2025). *Measuring digital development Facts and Figures.* ITU Publications. Retrieved 2026, from https://www.itu.int/itu-d/reports/statistics/facts-figures-2025/

Jacobson, B. R., Höne, K. E., & Kurbalija, J. (2018). *Data Diplomacy: Updating diplomacy to the big data era.* Geneva: DiploFoundation. Retrieved from https://www.diplomacy.edu/wp-content/uploads/2019/07/Data_Diplomacy_Report_2018.pdf

Jahangir, R. (2025, November 10). *EU Set the Global Standard on Privacy and AI. Now It's Pulling Back*. Retrieved January 2026, from TechPolicy.press: https://www.techpolicy.press/eu-set-the-global-standard-on-privacy-and-ai-now-its-pulling-back/

James, L. (2025, September 7). *Multiple undersea cable cuts in the Red Sea, hampering internet performance — international cables connecting Europe, Asia, and the Middle East are compromised*. Retrieved 2025, from Tom's hardware:

https://www.tomshardware.com/tech-industry/red-sea-cable-cut-takes-azure-routes-down

Jiang, C., & Martin, S. (2020). *The Geopolitics of Data Governance, Research Report Part I: Data Governance Regimes.* Oxford Insights. Retrieved from https://oxfordinsights.com/wp-content/uploads/2024/08/The-Geopolitics-of-Data-Governance_Oxford_insights_Master.pdf

Jung-joo, L. (2025, September 27). *Fire at government data center halts 647 systems, disrupts services*. Retrieved 2025, from The Korea Herald: https://www.koreaherald.com/article/10584785

Kanter, J. (2014, October 3). *Antitrust Nominee in Europe Promises Scrutiny of Big Tech Companies*. Retrieved January 2026, from The New York Times: https://archive.nytimes.com/bits.blogs.nytimes.com/2014/10/03/antitrust-nominee-in-europe-promises-eye-on-big-tech-companies/#:~:text=Policy-,Antitrust%20Nominee%20in%20Europe%20Promises%20Scrutiny%20of%20Big%20Tech%20Companies,deeper%20understanding%20of

Karacsony, E. (2025, September 22). Convergence in Grand Strategies: The France-UAE Partnership in AI. *ORF Issue Brief, No. 835*. Retrieved 2026, from Observer Research Foundation: https://orfme.org/research/convergence-in-grand-strategies-the-france-uae-partnership-in-ai/

Kasanmascheff, M. (2026, January 14). *Chinese Customs Block NVIDIA H200 Shipments Hours After US Approval, Freezing $54B in Orders*. Retrieved January 14, 2026, from WinBuzzer: https://winbuzzer.com/2026/01/14/chinese-customs-block-nvidia-h200-shipments-hours-after-us-approval-freezing-54b-in-orders-xcxwbn/?_bhlid=8fc8aed5f3f405ca22946506569166a6dc73f26b

Krantz, T., & Jonker, A. (2025). *What is a data product?* Retrieved from IBM: https://www.ibm.com/think/topics/data-product

Kurbalija, J. (2025, June 5). *Diplomatic Lexicon: A Guide to Hundreds Diplomatic Practices and Concepts [Coming soon]*. Retrieved from Diplo: https://www.diplomacy.edu/resource/diplomacy-decoded-300-types-diplomacy-explained/

Leblond, P. (2024, November 12). *Trade Agreements and Data Governance*. Retrieved 2025, from CIGI: https://www.cigionline.org/articles/trade-agreements-and-data-governance/

Lee, J. (2023, September 15). *ASEAN's Window of Opportunity for Shaping Global Data Governance*. Retrieved 2026, from The Diplomat: https://thediplomat.com/2023/09/aseans-window-of-opportunity-for-shaping-global-data-governance/

Lehdonvirta, V., Wú, B., & Hawkins, Z. (2025, April 21). Weaponised interdependence in a bipolar world: how economic forces and security interests shape the global reach of US and Chinese cloud data centres. *Review of International Political Economy, 32*(5), 1442-1467. doi:10.1080/09692290.2025.2489077

Library of Congress. (n.d.). *Oil and Gas Industry: A Research Guide*. Retrieved January 5, 2026, from Library of Congress: https://guides.loc.gov/oil-and-gas-industry/companies

Lloyd, N. (2025, November 27). *New research reveals algorithms' hidden political power*. Retrieved January 2026, from Northeastern Global News: https://news.northeastern.edu/2025/11/27/social-media-political-polarization-research/

Lu, M. (2025, November 19). *Visualizing All of the World's Data Centers in 2025*. Retrieved 2026, from Visual Capitalist: https://www.visualcapitalist.com/visualizing-all-of-the-worlds-data-centers-in-2025/

Mackinder, H. J. (1904, April). The Geographical Pivot of History. *The Geographical Journal, 23*(4), 421-437. Retrieved January 2026, from http://www.jstor.org/stable/1775498

Marr, B. (2015, February 25). *A brief history of big data everyone should read*. Retrieved from World Economic Forum: https://www.weforum.org/stories/2015/02/a-brief-history-of-big-data-everyone-should-read/

Marr, B. (n.d.). *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*. Retrieved from Bernard Marr & Co. : https://bernardmarr.com/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/

McBride, J., Berman, N., & Chatzky, A. (2023, February 2). *Council on Foreign Relations*. Retrieved 2026, from China's Massive Belt and Road Initiative: https://www.cfr.org/backgrounders/chinas-massive-belt-and-road-initiative

McKinsey. (2022, August 17). *What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?* Retrieved January 2026, from McKinsey & Company: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir

Mickle, T. (2025, July 10). *Nvidia Becomes First Public Company Worth $4 Trillion*. Retrieved 2025, from The New York Times: https://www.nytimes.com/2025/07/10/technology/nvidia-4-trillion-market-value.html

Microchip USA. (2025, March 15). *The Intersection of AI and Semiconductors*. Retrieved from MicrochipUSA.com: https://www.microchipusa.com/industry-news/the-intersection-of-ai-and-semiconductors-advancements-implications-and-future-opportunities?srsltid=AfmBOopl3J0w1wJBcbsXw3B6acOmmey9V5wLHDTn-R76O-3py1HwB3hd

Montgomery, E. (2025, November 11). *Top 6 Biggest State-Owned Oil Companies in the World*. Retrieved from hexn*: https://hexn.io/blog/top-6-biggest-state-owned-oil-companies-in-the-world-ppi9tj6hcvlrvnq2aq6d49hx

Navarro, P. (2018, December 10). *Why Economic Security Is National Security*. Retrieved from The White House archives: https://trumpwhitehouse.archives.gov/articles/economic-security-national-security/

Ndemo, B. (2024, August 8). *Addressing digital colonialism: A path to equitable data governance*. Retrieved November 2025, from UNESCO Inclusive Policy Lab: https://en.unesco.org/inclusivepolicylab/analytics/addressing-digital-colonialism-path-equitable-data-governance

Nicol-Schwarz, K. (2026, February 13). *These four charts show how reliant Europe is on U.S. digital infrastructure*. Retrieved from CNBC: https://www.cnbc.com/2026/02/13/four-charts-europes-reliance-us-digital-infrastructure.html

NODE. (2020, July 23). *Data is the new water*. Retrieved January 2026, from NODE: https://www.node-magazine.com/articles/data-is-the-new-water

Noureddine, R. (2016, November 24). *Critically assess and analyse the notion that the EU is a Normative Power.* Retrieved 2026, from EEAS: https://www.eeas.europa.eu/node/15687_en

Osborn, P. (2025, November-December). The restructuring of power and societies globally. *POLICY Journal*(10), pp. 8-28. Retrieved 2026

Pavić, A. M., Beriša, H. A., & Stajković, N. S. (2025). Trends in the formulation of instruments of national power: Digital diplomacy as a factor of change in modern diplomacy. *SCIENCE International journal, 4*(1), 25-33. doi:10.35120/sciencej0401025p

Pesce, M. (2024, November 20). *Data is the new uranium – incredibly powerful and amazingly dangerous*. Retrieved January 9, 2026, from The Register: https://www.theregister.com/2024/11/20/data_is_the_new_uranium/

Peters, B. (2012, June 21). *The Big Data Gold Rush*. Retrieved 2025, from Forbes: https://www.forbes.com/sites/bradpeters/2012/06/21/the-big-data-gold-rush/

Platias, A. G., & Constantopoulos, I. L. (2025, November-December). The dangerously interconnected world - geoeconomic competition and weaponisation of economic interdependence. *POLICY Journal*(10), pp. 29-41. Retrieved 2026

PromethEUs . (2023). *Joint Publication on EU Data Strategy: The EU's Data Strategy from a multifaceted perspective. Views from Southern Europe.* Retrieved 2025, from https://www.prometheusnetwork.eu/publications/prometheus-publication-eu-data-strategy-a-multifaceted-perspective-from-southern-european-countries/

Ricart, R. J. (2025, January 30). *Priorities for the international agenda of EU's digital policy in the 2024-2029 mandate*. Retrieved January 2026, from Elcano Royal Institute: https://www.realinstitutoelcano.org/en/work-document/priorities-for-the-international-agenda-of-eus-digital-policy-in-the-2024-2029-mandate/

Ritchie, H., Mathieu, E., Roser, M., & Ortiz-Ospina, E. (2023). Data Page: Share of the population using the Internet. *Internet*. Retrieved 2026, from Our World in Data: https://archive.ourworldindata.org/20250909-093708/grapher/share-of-individuals-using-the-internet.html

Ritchie, H., Mathieu, E., Roser, M., & Ortiz-Ospina, E. (2023). *Internet.* Retrieved January 2026, from OurWorldinData.org: https://ourworldindata.org/internet

Rocca, R., Tamagnone, N., Fekih, S., Contla, X., & Rekabsaz, N. (2023). Natural language processing for humanitarian action: Opportunities, challenges and the path toward humanitarian NLP. *Frontiers in Big Data, 6*. doi:10.3389/fdata.2023.1082787

Rosenbach, E., & Mansted, K. (2019). *The Geopolitics of Information.* Harvard Kennedy School, Belfer Center for Science and International Affairs, Cambridge, MA.

Rossi, B. (2015, August 21). *Data revolution: the gold rush of the 21st century*. Retrieved 2025, from Information Age: https://www.information-age.com/data-revolution-gold-rush-21st-century-2-32648/

Sacks, S. (2018, June 18). *Beijing Wants to Rewrite the Rules of the Internet*. Retrieved January 2026, from The Atlantic: https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/

Schlosser, A. (2018, January 10). *You may have heard data is the new oil. It's not*. Retrieved from World Economic Forum: https://www.weforum.org/stories/2018/01/data-is-not-the-new-oil/

Schrijver, N. (2008, June). *Natural Resources, Permanent Sovereignty over*. Retrieved January 2026, from Oxford Public International Law: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1442?d=%2F10.1093%2Flaw%3Aepil%2F9780199231690%2Flaw-9780199231690-e1442&p=emailA8C3Jmsf8XSzA&print#:~:text=This%20convention%20extended%20the%20breadth,Mankind;%20Internati

Singh, N. (2025, July 24). *Safeguarding Critical Infrastructure: Key Challenges in Global Cybersecurity*. Retrieved January 2026, from Carnegie: https://carnegieendowment.org/posts/2025/07/safeguarding-critical-infrastructure-key-challenges-in-global-cybersecurity?lang=en

Smyrnaios, N. (2018). *Internet Oligopoly - the corporate takeover of the digital world.* (C. J. Johnson, Trans.) Bingley: Emerald Publishing Limited.

Spindler, W., Fisher, L., & Atamian Hahn-Petersen, L. (2025, November 18). *Data centres use vast amounts of water – here's how we advance water circularity*. Retrieved from World Economic Forum: https://www.weforum.org/stories/2025/11/data-centres-and-water-circularity/

Stacciarini, J., & Gonçalves, R. (2025). *Data Centers, Critical Minerals, Energy, and Geopolitics: The Foundations of Artificial Intelligence.* doi:10.31235/osf.io/2zvkt_v1

Stryker, C. (n.d.). *What are large language models (LLMs)?* Retrieved January 09, 2026, from IBM: https://www.ibm.com/think/topics/large-language-models

Sundblad, W. (2018, October 18). *Data Is The Foundation For Artificial Intelligence And Machine Learning*. Retrieved from Forbes: https://www.forbes.com/sites/willemsundbladeurope/2018/10/18/data-is-the-foundation-for-artificial-intelligence-and-machine-learning/

Szczepański, M. (2020). *Is data the new oil? Competition issues in the digital economy.* European Parliamentary Research Service. European Parliamentary Research Service. Retrieved January 2026, from https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)646117

Taylor & Francis. (n.d.). *Yellowcake*. Retrieved 2026, from Taylor & Francis: https://taylorandfrancis.com/knowledge/Engineering_and_technology/Chemical_engineering/Yellowcake/

Taylor, J. (2024, January 26). *Data gold rush: companies once focused on mining cryptocurrency pivot to generative AI*. Retrieved 2026, from The Guardian: https://www.theguardian.com/australia-news/2024/jan/27/tech-companies-shift-generative-ai-chatgpt

Taylor, P. (2025, November 19). *Number of data centers worldwide as of November 2025, by country or territory*. Retrieved 2026, from Statista:

https://www.statista.com/statistics/1228433/data-centers-worldwide-by-country/?srsltid=AfmBOoqBdde3qdPD6Jl1IKJES93HCtGWHn-96OEt63u39gveFwtI5syM

The Economist. (2017, May 6). *Data is giving rise to a new economy*. Retrieved December 8, 2025, from The Economist: https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy

The Economist. (2017, May 6). *The world's most valuable resource is no longer oil, but data*. Retrieved from The Economist: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18151738051&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anony

Thibout, C. (2025, March 3). *When Trump defends his GAFAM*. Retrieved January 2026, from IRIS: https://www.iris-france.org/en/when-trump-defends-his-gafam/

Trachtenberg, D. M. (2025). *Digital Trade and Data Policy: Key Issues Facing Congress.* Congressional Research Service. Retrieved 2026, from https://www.congress.gov/crs-product/IF12347

Treverton, G. F., & Esfandiari, P. (2021, January 11). *Data: Governance and Geopolitics*. Retrieved November 11, 2025, from Center for Strategic & International Studies - CSIS: https://www.csis.org/analysis/data-governance-and-geopolitics

Tyson, M. (2025, September 11). *Taiwan increases defensive patrols around 24 undersea cables — closely monitoring '96 blacklisted China-linked boats' with 24-hour operations*. Retrieved 2025, from Tom's Hardware: https://www.tomshardware.com/networking/taiwan-increases-undersea-cable-protection-patrols-closely-monitoring-96-blacklisted-china-linked-boats

United Nations. (2024). *Pact for the Future, Global Digital Compact and Declaration on Future Generations.* New York: SUMMIT OF THE FUTURE OUTCOME DOCUMENTS.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. (2025). *2025 Technology and Innovation Report.* Geneva: United Nations. Retrieved from https://unctad.org/publication/technology-and-innovation-report-2025

United Nations Department of Economic and Social Affairs - Statistics . (n.d.). *UN World Data Forum*. Retrieved from Unstats: https://unstats.un.org/unsd/undataforum/

United Nations Environment Assembly of the United Nations Environment Programme. (2025). *UNEP/EA.7/INF/5 - Global Environmental Data Strategy.* Nairobi: United Nations. Retrieved from https://docs.un.org/en/UNEP/EA.7/INF/5

United Nations Environment Programme. (2024). *Artificial Intelligence (AI) end-to-end: The environmental impact of.* Nairobi. Retrieved January 2026, from https://wedocs.unep.org/items/5f3afe87-5419-439b-a6ee-14240b2605e9

United Nations Environmental Programme. (2025, June 12). *UNEP releases guidelines to curb the environmental impact of data centres*. Retrieved from UNEP.org: https://www.unep.org/technical-highlight/unep-releases-guidelines-curb-environmental-impact-data-centres

Vij, S., Warner, J., & Barua, A. (2020, June 21). Power in water diplomacy. *Water International, 45*(4), pp. 249-253. doi:10.1080/02508060.2020.1778833

World Economic Forum. (2017). *Exploring International Data Flow Governance.* Geneva. Retrieved January 2026, from https://www.weforum.org/publications/exploring-international-data-flow-governance/

Wriston, W. B. (1997, Sep-Oct). Bits, Bytes, and Diplomacy. *Foreign Affairs, 76*(5), pp. 172-182. Retrieved from https://www.jstor.org/stable/20048207

Wriston, W. B. (1997, September-October). Bits, Bytes, and Diplomacy. *Foreign Affairs, 76*(5), pp. 172-182. Retrieved 2025, from https://www.jstor.org/stable/20048207

Zhang, H., & Li, M. (2020, June 5). China's water diplomacy in the Mekong: a paradigm shift and the role of Yunnan provincial government. *Water International, 45*(4), 347-364. doi:10.1080/02508060.2020.1762369

Zuboff, S. (2019, August 15). Shoshana Zuboff on the Undetectable, Indecipherable World of Surveillance Capitalism. *Centre for International Governance Innovation*. (C. Tsalikis, Interviewer) Retrieved January 2026, from https://www.cigionline.org/articles/shoshana-zuboff-undetectable-indecipherable-world-surveillance-capitalism/